

103

THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1994

Y 4. G 74/7: H 34/13

The Fair Health Information Practic...

HEARINGS

BEFORE THE
INFORMATION, JUSTICE, TRANSPORTATION,
AND AGRICULTURE SUBCOMMITTEE
OF THE
COMMITTEE ON
GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRD CONGRESS
SECOND SESSION
ON
H.R. 4077

TO ESTABLISH A CODE OF FAIR INFORMATION PRACTICES FOR
HEALTH INFORMATION, TO AMEND SECTION 552A OF TITLE 5,
UNITED STATES CODE, AND FOR OTHER PURPOSES

APRIL 20, MAY 4 AND 5, 1994

Printed for the use of the Committee on Government Operations



THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1994

HEARINGS BEFORE THE INFORMATION, JUSTICE, TRANSPORTATION, AND AGRICULTURE SUBCOMMITTEE OF THE COMMITTEE ON GOVERNMENT OPERATIONS HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

ON

H.R. 4077

TO ESTABLISH A CODE OF FAIR INFORMATION PRACTICES FOR
HEALTH INFORMATION, TO AMEND SECTION 552A OF TITLE 5,
UNITED STATES CODE, AND FOR OTHER PURPOSES

APRIL 20, MAY 4 AND 5, 1994

Printed for the use of the Committee on Government Operations



U.S. GOVERNMENT PRINTING OFFICE

84-441 CC

WASHINGTON : 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

ISBN 0-16-046281-9

COMMITTEE ON GOVERNMENT OPERATIONS

JOHN CONYERS, JR., Michigan, *Chairman*

CARDISS COLLINS, Illinois
HENRY A. WAXMAN, California
MIKE SYNAR, Oklahoma
STEPHEN L. NEAL, North Carolina
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
JOHN M. SPRATT, JR., South Carolina
GARY A. CONDIT, California
COLLIN C. PETERSON, Minnesota
KAREN L. THURMAN, Florida
BOBBY L. RUSH, Illinois
CAROLYN B. MALONEY, New York
THOMAS M. BARRETT, Wisconsin
DONALD M. PAYNE, New Jersey
FLOYD H. FLAKE, New York
JAMES A. HAYES, Louisiana
CRAIG A. WASHINGTON, Texas
BARBARA-ROSE COLLINS, Michigan
CORRINE BROWN, Florida
MARJORIE MARGOLIES-MEZVINSKY,
Pennsylvania
LYNN C. WOOLSEY, California
GENE GREEN, Texas
BART STUPAK, Michigan

WILLIAM F. CLINGER, JR., Pennsylvania
AL McCANDLESS, California
J. DENNIS HASTERT, Illinois
JON L. KYL, Arizona
CHRISTOPHER SHAYS, Connecticut
STEVEN SCHIFF, New Mexico
CHRISTOPHER COX, California
CRAIG THOMAS, Wyoming
ILEANA ROS-LEHTINEN, Florida
RONALD K. MACHTLEY, Rhode Island
DICK ZIMMER, New Jersey
WILLIAM H. ZELIFF, JR., New Hampshire
JOHN M. McHUGH, New York
STEPHEN HORN, California
DEBORAH PRYCE, Ohio
JOHN L. MICA, Florida

BERNARD SANDERS, Vermont
(Independent)

JULIAN EPSTEIN, *Staff Director*
MATTHEW R. FLETCHER, *Minority Staff Director*

INFORMATION, JUSTICE, TRANSPORTATION AND AGRICULTURE SUBCOMMITTEE

GARY A. CONDIT, California, *Chairman*

MAJOR R. OWENS, New York
KAREN L. THURMAN, Florida
LYNN C. WOOLSEY, California
BART STUPAK, Michigan

CRAIG THOMAS, Wyoming
ILEANA ROS-LEHTINEN, Florida
STEPHEN HORN, California

EX OFFICIO

JOHN CONYERS, JR., Michigan

WILLIAM F. CLINGER, JR., Pennsylvania

ROBERT GELLMAN, *Chief Counsel*
AURORA OGG, *Clerk*
DIANE MAJOR, *Minority Professional Staff*

CONTENTS

	Page
Hearing held on:	
April 20, 1994	1
May 4, 1994	175
May 5, 1994	399
Text of H.R. 4077	15
Statement of:	
Baker, John, senior vice president, Equifax, Inc., Atlanta, GA	126
Barker, Richard, M.D., president, healthcare industries, IBM Corp., accompanied by Martin Sepulveda, M.D., director, occupational health services	316
Berenson, Aimee R., legislative counsel, AIDS Action Council	410
Bolan, Robert S., chairman, Medic Alert Foundation International, Turlock, CA	348
Condit, Hon. Gary A., a Representative in Congress from the State of California, and chairman, Information, Justice, Transportation, and Agriculture Subcommittee: Opening statement	1
Entin, Fredric, senior vice president and general counsel, American Hospital Association	221
Frawley, Kathleen, director, Washington office, American Health Information Management Association	291
Gimpel, Joel E., associate general counsel, Blue Cross and Blue Shield Association, Chicago, IL, representing the Workgroup on Electronic Data Interchange	250
Goldman, Janlori, director, privacy and technology project, American Civil Liberties Union	448
Hunter, Nan D., deputy general counsel, Department of Health and Human Services	104
Jacobs, Susan L., staff attorney, Legal Action Center, New York, NY	426
Lewers, Donald, M.D., member, board of trustees, American Medical Association	176
Sawyer, Hon. Thomas C., a Representative in Congress from the State of Ohio	399
Schwartz, Paul, associate professor of law, University of Arkansas Law School, Fayetteville, AR	358
Velázquez, Hon. Nydia, a Representative in Congress from the State of New York	95
Westin, Alan, professor of public law and government, Columbia University, New York, NY	152
Letters, statements, etc., submitted for the record by:	
Baker, John, senior vice president, Equifax, Inc., Atlanta, GA:	
Booklet entitled "Consumer Information and Privacy, the Equifax Perspective"	128
Prepared statement	139
Barker, Richard, M.D., president, healthcare industries, IBM Corp.: Prepared statement	320
Berenson, Aimee R., legislative counsel, AIDS Action Council: Prepared statement	413
Bolan, Robert S., chairman, Medic Alert Foundation International, Turlock, CA: Prepared statement	351
Condit, Hon. Gary A., a Representative in Congress from the State of California, and chairman, Information, Justice, Transportation, and Agriculture Subcommittee: Opening statement	2
Conyers, Hon. John, Jr., a Representative in Congress from the State of Michigan: Prepared Statement	94

IV

	Page
Letters, statements, etc., submitted for the record by—Continued	
Entin, Fredric, senior vice president and general counsel, American Hospital Association: Prepared statement	224
Frawley, Kathleen, director, Washington office, American Health Information Management Association: Prepared statement	293
Gimpel, Joel E., associate general counsel, Blue Cross and Blue Shield Association, Chicago, IL, representing the Workgroup on Electronic Data Interchange: Prepared statement	254
Goldman, Janlori, director, privacy and technology project, American Civil Liberties Union:	
Views concerning H.R. 4077	470
Prepared statement	451
Hunter, Nan D., deputy general counsel, Department of Health and Human Services: Prepared statement	109
Jacobs, Susan L., staff attorney, Legal Action Center, New York, NY: Prepared statement	429
Lewers, Donald, M.D., member, board of trustees, American Medical Association: Prepared statement	178
Owens, Hon. Major R., a Representative in Congress from the State of New York: Prepared statement	406
Sawyer, Hon. Thomas C., a Representative in Congress from the State of Ohio: Prepared statement	402
Schwartz, Paul, associate professor of law, University of Arkansas Law School, Fayetteville, AR: Prepared statement	362
Sepulveda, Martin, M.D., director, occupational health services, IBM Corp.: Prepared statement	320
Thomas, Hon. Craig, a Representative in Congress from the State of Wyoming: Prepared statement	405
Westin, Alan, professor of public law and government, Columbia University, New York, NY: Prepared statement	158
Woolsey, Hon. Lynn C., a Representative in Congress from the State of California: Prepared statement	103

APPENDIXES

Appendix 1.—Response to subcommittee questions by Ms. Patti Goldman, senior associate director, congressional and executive branch relations, American Hospital Association	479
Appendix 2.—Statements submitted for the record	499
Appendix 3.—Health information privacy survey 1993. Conducted for Equifax by Louis Harris and Associates in association with Dr. Alan Westin, Columbia University	532

THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1994

WEDNESDAY, APRIL 20, 1994

HOUSE OF REPRESENTATIVES,
INFORMATION, JUSTICE, TRANSPORTATION,
AND AGRICULTURE SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, DC.

The committee met, pursuant to notice, at 9:35 a.m., in room 2247, Rayburn House Office Building, Hon. Gary A. Condit (chairman of the subcommittee), presiding.

Present: Representatives Gary A. Condit, Lynn C. Woolsey, Craig Thomas, Ileana Ros-Lehtinen and Stephen Horn.

Also present: Representative John Conyers, Jr.

Staff present: Robert Gellman, chief counsel; Aurora Ogg, clerk; and Diane Major, minority professional staff, Committee on Government Operatons.

OPENING STATEMENT OF CHAIRMAN CONDIT

Mr. CONDIT. If I could have your attention, we'll begin the meeting. Today we're holding the first in a series of hearings on H.R. 4077, The Health Information Practice Act of 1994.

The purpose of the legislation is to establish a uniform Federal code of fair information practices for health data. The bill covers individually identifiable health information that originated or is used in the health treatment and payment process.

The need for Federal legislation was clearly established in a hearing held by this subcommittee last November. The Office of Technology Assessment reported that the present system of protecting health care information is based on a patchwork quilt of laws. State laws vary significantly in scope and Federal laws are applicable only to limited kinds of information.

I have a lengthy statement that I would like to add that gives an explanation of the bill and answers some questions that have been asked about the bill, and I will include that in the record and make that available to anyone who would like to review it.

[The opening statement of Mr. Condit and a copy of the bill H.R. 4077 follows:]

Opening Statement

CHAIRMAN GARY CONDIT

Subcommittee on Information, Justice, Transportation and Agriculture

FAIR HEALTH INFORMATION PRACTICES ACT OF 1994 (H.R. 4077)

April 20, 1994

Today we hold the first in a series of hearings on H.R. 4077, the Fair Health Information Practices Act of 1994. The purpose of the legislation is to establish a uniform federal code of fair information practices for health data. The bill covers individually identifiable health information that originates or is used in the health treatment and payment process.

The need for federal legislation was clearly established in a hearing held by this Subcommittee last November. The Office of Technology Assessment reported that the present system of protecting health care information is based on a patchwork quilt of laws. State laws vary significantly in scope, and federal laws are applicable only to limited kinds of information. *Overall, OTA found that the present legal scheme does not provide consistent, comprehensive protection for privacy in health care information.* Similar conclusions were reached by other witnesses and in other studies.

The need for legislation is even stronger now because of the prospect of health reform. Increased transfer and use of health information will be key elements in any health reform plan. Establishing rules that define the proper uses of identifiable health information is a necessary feature of health reform legislation. H.R. 4077 will provide a comprehensive, uniform, and reasonable set of guidelines that will be compatible with any health bill that passes the Congress.

Anyone who has ever looked at any health care legislation knows that it can be complex. H.R. 4077 is no exception. The health care system is large and complicated, involving many different institutions, organizations, and government agencies. Balancing the confidentiality interests of patients with the information needs of the health care system is not a simple task.

I believe that most Americans would be surprised -- and not especially pleased -- about the extensive use of health information for non-treatment purposes both inside and outside the health care system. As a practical matter, however, it is not possible to promise patients absolute privacy. But where use of health records must be tolerated, we can ask that users accept a greater responsibility as a condition of access. A code of fair information practices means that there will be some changes in the handling of patient data. Users will be accountable for the ways in which they use and disclose data.

I will not take the time now to describe H.R. 4077. Attached to my opening statement is a set of questions and answers with more information about the bill. We will certainly cover some of the specifics at these hearings.

The Subcommittee has scheduled two additional hearings next week, on Wednesday and Thursday. The witnesses will include representatives of some of the major health care organizations and advocacy groups. Those who cannot be accommodated at the hearings may submit written comments or testimony.

Today, we will hear from Rep. Nydia Velázquez, Representative from the Twelfth District of New York, and a cosponsor of the bill. She will share with us her own story about the improper disclosure of sensitive health information. We will also receive testimony from the Clinton Administration, represented by Nan Hunter, Deputy General Counsel at the Department of Health and Human Services.

Finally, we will hear the results of a recent public opinion poll on health privacy issues. Equifax has performed an important public service by sponsoring this very timely survey. Equifax is represented today by John Baker, Senior Vice President. The analysis will be provided by Professor Alan Westin of Columbia University. Professor Westin is one of the leading privacy scholars, and he conducted the first study on computers and health records in 1976.

Fair Health Information Practices Act of 1994 (H.R. 4077)

Executive Summary

The Fair Health Information Practices Act of 1994 (H.R. 4077) was introduced on March 17, 1994, by Rep. Gary Condit, Chairman of the Subcommittee on Information, Justice, Transportation, and Agriculture. The bill is intended to be considered as part of the Health Security Act (H.R. 3600). Subtitle B of Title V of the Health Security Act has been referred to the Subcommittee.

The purpose of the Act is to establish a code of fair information practices for the use and disclosure of health information that originates in or becomes a part of the health treatment or payment system. The Act establishes uniform federal rules that will apply to covered health information in all states.

There are two new basic concepts in the Act. First, identifiable health information relating to the provision of or payment for health care that is created or used during the medical treatment or payment process becomes *protected health information*. In general, protected health information remains subject to statutory restriction no matter how it is used or disclosed.

The second basic concept is that of a *health information trustee*. Almost anyone who has access to protected health information becomes a health information trustee under the bill. There are three different types of trustees. Those directly involved in providing treatment and in paying for treatment are *health use trustees*. Those who use identifiable information for public health or health research purposes are *public health trustees*. Finally, others who have an occasional need for health information to accomplish a specific purpose authorized by law are *special purpose trustees*.

Each class of trustee has a set of responsibilities and authorities that have been carefully defined to balance legitimate societal needs for data against each patient's right to privacy and the need for confidentiality in the health treatment process.

Trustees are required to --

- maintain appropriate administrative, technical, and physical safeguards to protect integrity and privacy of health information;
- maintain an accounting of the date, nature, and purpose of any disclosure of protected health information;

- use protected health information only for a purpose that is compatible with and related to the purpose for which the information was collected or obtained by the trustee;

- limit use or disclosure of protected health information to the minimum necessary to accomplish the purpose;

- disclose protected health information only for a purpose that is authorized by the Act. Permissible disclosures vary by trustee; health use trustees have the most authority and special purpose trustees the least.

Patient rights vary slightly depending on which type of trustee maintains protected health information. For health information used in treatment or payment, patients have the right to --

- inspect and to have a copy of medical information about themselves;

- seek correction of health information about themselves that is not timely, accurate, relevant, or complete.

- receive a notice of information practices describing their rights, the procedures for the exercise of those rights, and the disclosures of health information that are authorized.

The Fair Health Information Practices Act of 1994 includes several different enforcement mechanisms. There are criminal penalties (up to ten year in prison), civil remedies for aggrieved patients, and civil money penalties that may be imposed by the Secretary of Health and Human Services. In addition, the Act provides for alternate dispute resolution as another mechanism for resolving disputes between patients and health information trustees.

Fair Health Information Practices Act of 1994 (H.R. 4077)**Frequently Asked Questions****1. What does the Fair Health Information Practice Act of 1994 do?**

The Fair Health Information Practices Act will be the first federal law that governs the use of all health records throughout the United States. The bill --

- establishes uniform, comprehensive federal rules governing the use and disclosure of identifiable health information about individuals
- specifies the responsibilities of those who collect, use, and maintain health information about patients
- defines the rights of patients
- provides mechanisms that will allow patients to enforce their rights

2. What are the highlights of the bill?

- A new culture for health information emphasizing fair information practices
- Comprehensive rules for health information that follow the information when it is disclosed to secondary users outside the treatment and payment process
- Patient rights of access and correction
- Effective enforcement mechanisms, including major criminal penalties (up to ten years) for violations
- Limits on how much health information can be disclosed

3. Why do we need a federal law for health records?

In a recent report titled Protecting Privacy in Computerized Medical Information, the Office of Technology Assessment found that the present system of protecting health care information is based on a patchwork quilt of laws. There are state laws of varying scope and federal laws applicable to limited kinds of information or to information maintained only by the federal government. Overall, OTA found that *the present legal scheme does not provide consistent, comprehensive protection for privacy in health care information, whether that information exists in a paper or computerized environment.* Health reform and increased computerization make it imperative that doctors, insurance companies, and others operate under the same set of rules.

4. What are fair information practices?

Fair information practices describe a set of rules for handling personal information. The concept was developed by a federal advisory committee in 1973, and the basic principles were implemented in the Privacy Act of 1974, a law that applies to personal records maintained by federal agencies. Fair information practices have been adopted all over the world as the basis for privacy or data protection laws. Fair information practices include the access to records, correction of records, limits on use and disclosure of personal information, security, and accountability for record keepers.

5. What kind of health information will be covered by the Act?

Protected health information is defined in the bill to include individually identifiable data related to the health of a patient, the provision of health care to a patient, or the payment for health care to a patient. In essence, information is covered if it is created during or becomes part of the treatment or payment process.

6. Does this mean that all health information about an individual is protected?

No. Health information becomes protected health information when it is created by or is in the possession of a *health information trustee*. Information held by those who are not health information trustees is not covered. If you tell a friend that you have a cold, there are no federal confidentiality requirements imposed on that friend. But when a health information trustee discloses information under the Act, the information will remain subject to the Act in the hands of most recipients. This will plug a major loophole in current law. Today, information that may be protected in the hands of a doctor may not be protected when disclosed to an insurance company.

7. What is a health information trustee?

There are three classes of health information trustee.

- A *health care trustee* is a health care provider, insurer, or a health oversight agency.
- A *public health trustee* is a federal or state public health authority or a person conducting biomedical, epidemiologic, or health services research that has been approved by an Institutional Review Board.
- A *special purpose trustee* is a person who is permitted to obtain protected health information for emergency purposes; for a judicial, administrative or legally required reporting purposes; for narrowly defined law enforcement purposes; or pursuant to a subpoena or search warrant.

8. Why are there three different trustees?

Institutions maintain and use health information for different reasons. For example, information may be used for treatment, for protection of the public health, for law enforcement, in emergencies, and in other ways. But not every user of health data needs to use it in the same way. A doctor will need to make some uses that will not apply to a public health worker. When a law enforcement authority is able to obtain health records, a patient may require special protections that are not necessary when the same information is held by a doctor.

The trustee structure allows every authorized user to have no more authority than is needed to carry out that user's purpose. This affords much more specific protection for health information than a one-size-fits-all approach.

9. What are the general responsibilities of health information trustees?

- *Limited Use Rule:* All trustees are required to use protected health information only for a purpose that is compatible with and related to the purpose for which the information was collected or obtained by the trustee.
- *Limited Disclosure Rule:* All trustees are permitted to disclose protected health information only for a purpose that is authorized by the Act.
- *Minimal Disclosure Rule:* All trustees are required to limit use or disclosure of protected information to the minimum necessary to accomplish the purpose.
- *Accounting for Disclosure Rule:* All trustees are required to maintain an accounting for any disclosures of protected health information.
- *Security Rule:* All trustees are required to maintain appropriate administrative, technical, and physical safeguards for protected health information.

10. What rights does a patient have?

For protected health information in the possession of a health use trustee, a patient has the right to inspect and seek correction of the information. Information can be withheld from the patient only under a few narrowly defined circumstances. In addition, a patient has a right to obtain a notice of information practices describing in detail the rights of the patient and how the information may be used and disclosed.

11. When can a health information trustee disclose information to others?

Different trustees have different authority to disclose information. Health use trustees have the greatest authority to disclose data. There is less need for public health trustees to disclose identifiable information, and the authority of public health trustees is more limited. Special purpose trustees are even more restricted.

Authorized disclosures are permissive and not mandatory. This means that a trustee authorized to make a disclosure under the Act is not required to make the disclosure unless another law so requires. This generally permits trustees to exercise discretion when disclosing information.

The following chart explains when health information trustees are authorized to disclose protected health information:

TRUSTEES =====>	Health Use	Public Health	Special Purpose
Authority to Disclose:			
Patient Authorization	Y	Y	Y
Treatment, Payment, Oversight	Y	N	N
Next of Kin, Directory Info.	Y	N	N
Public Health	Y	Y	N
Emergency Circumstances	Y	Y	Y
Judicial, Administrative and Legally Required Reporting	Y	N	N
Health Research	Y	Y	N
Law Enforcement	Y	Y	Y
Subpoenas and Warrants	Y	N	Y

12. When can a health information trustee share information with employees, contractors, affiliates, and subsidiaries?

Sharing information with contractors and other affiliated persons is permitted subject to the general rule that access must be limited to the minimum amount of information necessary to accomplish the purpose. Affiliated persons have no more authority than the trustee, and the trustee is required to define the extent to which duties and authorities under the Act are transferred, shared, or retained by the trustee. Health care providers may utilize contractors as they do today; protected health information remains subject to the Act in the hands of contractors; and patients' rights continue to be protected.

13. How can an employer use protected health information about an employee?

An employer is likely to acquire protected health information about an employee in two ways. First, an employer may provide treatment through a first aid station or the equivalent. Second, an employer may be involved in the processing of insurance claims. In either case, the employer will become a health care provider and will be subject to the rules for health care providers, including the requirement to limit access to and disclosure of protected health information. Use of information about employees for purposes unrelated to treatment or payment will not be permitted. Thus, an employer will not be able to take information from insurance claims and use it for making decisions about employee assignments or promotions. Nothing in the bill is inconsistent with or will disturb the rules of the Americans with Disability Act regulating employer use of health information.

14. When can a patient see his or her own health records?

Any health care provider (principally providers and insurers) must permit a patient to see his or her own information. A patient may inspect and obtain a copy of the information. Information can be withheld from a patient only if it is confidential psychiatric notes; relates to another individual and access would be harmful; disclosure would endanger life or safety of an individual; would identify a confidential source; is solely administrative or duplicative; or was compiled in anticipation of litigation.

15. What security measures are required?

The bill does not specify the technical security measures that are needed. The bill requires "appropriate administrative, technical, and physical safeguards." What is appropriate depends on which technology is used to store information (e.g., paper, computers, networks) and on the state of the art. As better security measures are developed, they can be implemented without the need for amendments to the law. For example, encryption may be one of the security measures that is eventually used routinely when communicating protected health information.

The Act does require several specific security measures. These are employee training in confidentiality rules; audit trails whenever practicable; and the posting of signs and warnings about the need to protect confidential information. It will be up to trustees to determine how to carry out these requirements.

16. Will patients be asked to authorize routine disclosures?

The Act permits a health care provider to disclose information to another health care provider for use in treatment or payment without specific authorization from the patient. Patients may veto disclosures for treatment, and they may make alternate arrangements that would include limiting disclosures for payment. For the majority of patients, however, these disclosures will be routine -- just as they are today -- and can be made without formal authorization. The advantage of this approach is that the bill's strict limits apply to information disclosed in this fashion. Disclosures made through authorizations are not as expressly controlled because the patient has agreed to the terms of the disclosure. Under the bill, patients with special confidentiality concerns will have the tools and the ability to seek and to enforce special use and disclosure arrangements.

By limiting requirements for patient authorizations, it is expected that authorizations will become relatively rare. Patients will learn to scrutinize requests for authorization more closely. Also, information disclosed directly under the Act's provisions will remain subject to the fair information practices in the hands of the recipient. This will greatly enhance protections for health information.

There are strict rules governing authorizations for disclosure, including electronic authorizations. The ability of trustees to seek authorizations is limited in order to prevent inadvertent, uninformed, or automatic authorizations from being obtained.

17. When can protected health information lose its protection under the Act?

The general rule is that protected health information remains subject to the Act when it is disclosed to a third party. This is a major advance in the protection of health records and fills a significant loophole in virtually all existing confidentiality rules. There are only a few circumstances in which protected health information is disclosed to a third party and does not remain subject to protection.

- Directory information (name, location, and general condition) may be disclosed if the patient has not objected and if the disclosure does not reveal specific information about a patient's condition or treatment. When directory information is disclosed, the information is not protected in the hands of the recipient.
- Information may be disclosed to a patient's next of kin if the patient has not objected and the disclosure is consistent with accepted medical practice. When information is disclosed under this authority, the information is not protected in the hands of the recipient.
- Information disclosed by or under the authority of a patient (other than to a health information trustee) is not protected in the hands of the recipient. But limitations agreed to in the authorization form are binding on the recipient.

The policy reflected here is that the Act does not impose confidentiality duties on casual recipients of health information who are not likely to be aware of duties. For example, an individual will not be subject to a lawsuit for telling a spouse that a neighbor has a cold.

18. When can a health researcher obtain protected health information?

A health researcher can only obtain identifiable health information about patients if the research project has been approved by an Institutional Review Board (IRB). The IRB must first find that the research is of sufficient importance so as to outweigh the intrusion into patient privacy that would result from the disclosure. The IRB must also find that it is reasonably impracticable to conduct the research without identifiers.

A researcher who clears these hurdles and receives protected health information is a public health trustee. The researcher thereby becomes subject to the rules of the Act and has enforceable responsibilities to protect patient information. In addition, the Act requires researchers to remove or destroy identifiers at the earliest opportunity consistent with the purposes of the project.

19. What law enforcement disclosures are permitted?

There are limited circumstances in which a health information trustee can make disclosures of protected health information to a law enforcement agency. The authority for these disclosures is narrowly defined, subject to procedural requirements to assure accountability, and accompanied by strict limits against use of the information in a way that is unfair to a patient.

- Information may be disclosed for use in an investigation or prosecution of a trustee (but not a patient). This facilitates civil or criminal investigations of trustees when patients are not the subject of the investigation. This also prevents trustees from hiding improper conduct by invoking the privacy rights of patients.
- Information may be disclosed to assist in the identification or location of a suspect, fugitive, or witness in a law enforcement inquiry. This prevents hospitals from becoming sanctuaries for individuals attempting to evade the law.
- Information may be disclosed in connection with criminal activity committed against a trustee. This permits hospitals, for example, to report criminal conduct by patients.
- Information may be disclosed to determine if a crime has been committed (other than a crime that may have been committed by a patient). If a patient is a victim of a crime, necessary information may be disclosed.

Disclosures for law enforcement purposes are subject to the general rule that the information disclosed must be limited to the minimum necessary to accomplish the purpose. In addition, the law enforcement agency seeking the information must provide a written certification signed by a supervisory official specifying the information requested and stating that it is being sought for a lawful purpose. This assures accountability.

There are two additional protections. First, information obtained under this procedure may not be used against the patient in any administrative, civil, or criminal action or investigation, except in an action or investigation arising out of and directly related to the action or investigation for which the information was obtained. A patient engaged in fraud against the health system will not be protected, but any other use of the patient's health information will be prevented.

Second, the information obtained under this procedure may not be otherwise used or disclosed unless necessary to fulfill the purpose for which the information was obtained. This protects patients from the use of confidential information in investigatory fishing expeditions.

20. Can protected health information be subpoenaed?

Yes, but only with procedural safeguards that provide notice to patients and that permit them effectively to assert their rights in court. A patient who is a party to litigation already has the capability of protecting his or her rights. The Act offers additional protections against the use of compulsory process in cases where the patient is not a party to ongoing litigation.

When protected health records are sought by the government or by private litigants, the patient who is the subject of the records must be notified of the subpoena. The patient can then object to the subpoena in court. The Act establishes standards that the person seeking the information must meet, and gives the patient an identifiable statutory interest that can be asserted to defeat the subpoena. A judge is required to balance the requester's need for information against the patient's privacy interest.

21. Will the Act prevent disease reporting to public health authorities?

No. Protected health information may continue to be reported to public health authorities for use in disease reporting, public health surveillance, or public health investigations. In addition, other laws requiring the reporting of gunshot wounds and similar conditions to law enforcement authorities are not affected. The Act does provide, however, that the recipients of this information become health information trustees and have the responsibility to maintain the information in accordance with the fair information practices standards of the Act.

22. Will federal health records be subject to the new Fair Health Information Practices Act or to the existing Privacy Act of 1974?

Federal health records will be fully subject to the new law, just like records maintained by others. A few current requirements of the Privacy Act of 1974 -- such as the provision mandating publication of a description of a system of records -- will continue to apply. These requirements will supplement and not modify or supersede any of the provisions of the Fair Health Information Practices Act.

23. How does the Fair Health Information Practices Act compare to existing rules governing use of information of alcohol and drug abuse treatment?

This is a good example of how the comprehensiveness of the new Act generally offers better protection for health information than existing special treatment laws. While the laws and the proposed Act are not completely analogous, a comparison of the existing statute with the proposed Act shows:

- Violations of the drug and alcohol laws are punishable by a fine of \$500 to \$5000. The new Act has more severe criminal penalties, with prison sentences of up to ten years and fines up to \$250,000. In addition, the new Act provides civil remedies and administrative sanctions.
- Drug and alcohol laws permit disclosures to researchers, auditors, and program evaluators. The new Act supports these disclosures under more specified conditions. In addition, the new Act requires identification of all protected health information when disclosed. It also regulates use and restricts redisclosure of information by third-party recipients.
- Access to drug and alcohol records is permitted by court order for "good cause". The new Act normally requires actual notice to the patient before a subpoena can be enforced, requires a more specific showing by the person seeking the information, and gives the patient a greater protectable interest in the information. The result is a higher barrier to access.

- The drug and alcohol laws prohibit use of information to initiate or substantiate any criminal charges or to conduct any investigation against a patient. The new Act generally prohibits use of information in any administrative, civil, or criminal action or investigation against a patient.

- The proposed Act establishes general rules protecting all health information, including specific requirements for patient authorizations, access by the patient, accounting for disclosures, security. There are no comparable requirements in drug and alcohol statutes, although the regulations include some similar, but generally weaker, provisions.

In general, protection of especially sensitive health information is more effective without special rules, labelling, or handling because neither records nor patients are stigmatized or identified by the special treatment.

103D CONGRESS
2D SESSION

H. R. 4077

To establish a code of fair information practices for health information, to amend section 552a of title 5, United States Code, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 17, 1994

Mr. CONDIT (for himself, Mr. CONYERS, and Ms. VELÁZQUEZ) introduced the following bill; which was referred jointly to the Committees on Government Operations, the Judiciary, and Energy and Commerce

A BILL

To establish a code of fair information practices for health information, to amend section 552a of title 5, United States Code, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the
5 “Fair Health Information Practices Act of 1994”.

6 (b) **TABLE OF CONTENTS.**—The table of contents for
7 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings and purposes.
- Sec. 3. Definitions.

TITLE I—FAIR INFORMATION PRACTICES FOR PROTECTED
HEALTH INFORMATION

Subtitle A—Treatment of Protected Health Information

- Sec. 101. Duties and authorities of health use trustees.
- Sec. 102. Duties and authorities of public health trustees.
- Sec. 103. Duties and authorities of special purpose trustees.
- Sec. 104. Duties and authorities of affiliated persons.

Subtitle B—Duties and Authorities of Health Information Trustees

PART 1—DUTIES OF HEALTH INFORMATION TRUSTEES

- Sec. 111. Inspection of protected health information.
- Sec. 112. Amendment of protected health information.
- Sec. 113. Notice of information practices.
- Sec. 114. Accounting for disclosures.
- Sec. 115. Security.

PART 2—USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

- Sec. 121. General limitations on use and disclosure.
- Sec. 122. Authorizations for disclosure of protected health information.
- Sec. 123. Treatment, payment, and oversight.
- Sec. 124. Next of kin and directory information.
- Sec. 125. Public health.
- Sec. 126. Emergency circumstances.
- Sec. 127. Judicial, administrative, and other legal purposes.
- Sec. 128. Health research.
- Sec. 129. Law enforcement.
- Sec. 130. Subpoenas, warrants, and search warrants.

Subtitle C—Access Procedures and Challenge Rights

- Sec. 141. Access procedures for law enforcement subpoenas, warrants, and search warrants.
- Sec. 142. Challenge procedures for law enforcement subpoenas.
- Sec. 143. Access and challenge procedures for other subpoenas.
- Sec. 144. Construction of subtitle; suspension of statute of limitations.
- Sec. 145. Responsibilities of Secretary.

Subtitle D—Miscellaneous Provisions

- Sec. 151. Debit and credit card transactions.
- Sec. 152. Access to protected health information outside of the United States.
- Sec. 153. Standards for electronic documents and communications.
- Sec. 154. Powers of attorney.
- Sec. 155. Rights of incompetents.
- Sec. 156. Rights of minors.

Subtitle E—Enforcement

- Sec. 161. Civil actions.
- Sec. 162. Civil money penalties.
- Sec. 163. Alternative dispute resolution.
- Sec. 164. Amendments to criminal law.

TITLE II—AMENDMENTS TO TITLE 5, UNITED STATES CODE

Sec. 201. Amendments to title 5, United States Code.

TITLE III—REGULATIONS; EFFECTIVE DATES; APPLICABILITY;
AND RELATIONSHIP TO OTHER LAWS

Sec. 301. Regulations.

Sec. 302. Effective dates.

Sec. 303. Applicability.

Sec. 304. Relationship to other laws.

1 SEC. 2. FINDINGS AND PURPOSES.

2 (a) FINDINGS.—The Congress finds as follows:

3 (1) The right to privacy is a personal and fun-
4 damental right protected by the Constitution of the
5 United States.

6 (2) The improper use or disclosure of personally
7 identifiable health information about an individual
8 may cause significant harm to the interests of the
9 individual in privacy and health care, and may un-
10 fairly affect the ability of the individual to obtain
11 employment, education, insurance, credit, and other
12 necessities.

13 (3) Current legal protections for health infor-
14 mation vary from State to State and are inadequate
15 to meet the need for fair information practices
16 standards.

17 (4) The movement of individuals and health in-
18 formation across State lines, access to and exchange
19 of health information from automated data banks
20 and networks, and the emergence of multistate

4

1 health care providers and payors create a compelling
2 need for uniform Federal law, rules, and procedures
3 governing the use, maintenance, and disclosure of
4 health information.

5 (5) Uniform rules governing the use, mainte-
6 nance, and disclosure of health information are an
7 essential part of health care reform, are necessary to
8 support the computerization of health information,
9 and can reduce the cost of providing health services
10 by making the necessary transfer of health informa-
11 tion more efficient.

12 (6) An individual needs access to health infor-
13 mation about the individual as a matter of fairness,
14 to enable the individual to make informed decisions
15 about health care, and to correct inaccurate or in-
16 complete information.

17 (b) PURPOSES.—The purposes of this Act are as
18 follows:

19 (1) To define the rights of an individual with
20 respect to health information about the individual
21 that is created or maintained as part of the health
22 treatment and payment process.

23 (2) To define the rights and responsibilities of
24 a person who creates or maintains individually iden-

1 tifiable health information that originates or is used
2 in the health treatment or payment process.

3 (3) To establish effective mechanisms to enforce
4 the rights and responsibilities defined in this Act.

5 **SEC. 3. DEFINITIONS.**

6 (a) DEFINITIONS RELATING TO PROTECTED
7 HEALTH INFORMATION.—For purposes of this Act:

8 (1) DISCLOSE.—The term “disclose”, when
9 used with respect to protected health information,
10 means to provide access to the information, but only
11 if such access is provided by a health information
12 trustee to a person other than—

13 (A) the trustee or an officer or employee of
14 the trustee;

15 (B) an affiliated person of the trustee; or

16 (C) the individual who is the subject of the
17 information.

18 (2) DISCLOSURE.—The term “disclosure”
19 means the act or an instance of disclosing.

20 (3) PROTECTED HEALTH INFORMATION.—The
21 term “protected health information” means any in-
22 formation, whether oral or recorded in any form or
23 medium, that—

1 (A) is created or received by a health use
2 trustee or a public health trustee in a State;
3 and

4 (B) relates to the past, present, or future
5 physical or mental health of an individual, the
6 provision of health care to an individual, or
7 payment for the provision of health care to an
8 individual and—

9 (i) identifies the individual; or

10 (ii) with respect to which there is a
11 reasonable basis to believe that the infor-
12 mation can be used readily to identify the
13 individual.

14 (b) DEFINITIONS RELATING TO HEALTH INFORMA-
15 TION TRUSTEES.—For purposes of this Act:

16 (1) HEALTH BENEFIT PLAN.—The term
17 “health benefit plan” means any public or private
18 entity or program that provides payments for health
19 care—

20 (A) including—

21 (i) a group health plan (as defined in
22 section 607 of the Employee Retirement
23 Income Security Act of 1974) or a multiple
24 employer welfare arrangement (as defined

1 in section 3(40) of such Act) providing
2 health benefits; and

3 (ii) any other health insurance ar-
4 rangement, including any arrangement
5 consisting of a hospital or medical expense
6 incurred policy or certificate, hospital or
7 medical service plan contract, or health
8 maintenance organization subscriber con-
9 tract;

10 (B) but not including—

11 (i) an individual making payment on
12 the individual's own behalf (or on behalf of
13 a relative or other individual) for health
14 care or for deductibles, coinsurance,
15 copayments, items, or services not covered
16 under a health insurance arrangement;

17 (ii) a plan sponsor (as defined in sec-
18 tion 3(16) of the Employee Retirement In-
19 come Security Act of 1974);

20 (iii) an employer of an employee cov-
21 ered under a multiple employer welfare
22 arrangement;

23 (iv) an employee organization that
24 sponsors a multiple employer welfare
25 arrangement; or

1 (v) an organization, association, com-
2 mittee, joint board of trustees, or similar
3 group of representatives of 2 or more em-
4 ployers described in clause (iii) or 2 or
5 more employee organizations described in
6 clause (iv).

7 (2) HEALTH CARE PROVIDER.—The term
8 “health care provider” means a person who is li-
9 censed, certified, registered, or otherwise authorized
10 by law to provide an item or service that constitutes
11 health care in the ordinary course of business or
12 practice of a profession.

13 (3) HEALTH INFORMATION TRUSTEE.—The
14 term “health information trustee” means a person
15 who—

16 (A) creates or receives protected health in-
17 formation that affects interstate commerce; and

18 (B) is a health use trustee, public health
19 trustee, or special purpose trustee.

20 (4) HEALTH OVERSIGHT AGENCY.—The term
21 “health oversight agency” means a person—

22 (A) who performs or oversees the perform-
23 ance of an assessment, evaluation, determina-
24 tion, or investigation relating to the licensing,

1 accreditation, or certification of health care
2 providers;

3 (B) who—

4 (i) enters into agreements with health
5 benefit plans that are offered to individuals
6 residing in a specific geographic region in
7 order to facilitate the enrollment of such
8 individuals in such plans; and

9 (ii) is a public agency, acting on be-
10 half of a public agency, acting pursuant to
11 a requirement of a public agency, or carry-
12 ing out activities under a State or Federal
13 statute regulating the agreements; or

14 (C) who—

15 (i) performs or oversees the perform-
16 ance of an assessment, evaluation, deter-
17 mination, or investigation relating to the
18 effectiveness of, compliance with, or appli-
19 cability of, legal, fiscal, medical, or sci-
20 entific standards or aspects of performance
21 related to the delivery of, or payment for,
22 health care; and

23 (ii) is a public agency, acting on be-
24 half of a public agency, acting pursuant to
25 a requirement of a public agency, or carry-

1 ing out activities under a State or Federal
2 statute regulating the assessment, evalua-
3 tion, determination, or investigation.

4 (5) HEALTH RESEARCHER.—The term “health
5 researcher” means a person who conducts a health
6 research project.

7 (6) HEALTH USE TRUSTEE.—The term “health
8 use trustee” means a person who, with respect to
9 protected health information, receives, creates, uses,
10 maintains, or transmits such information while act-
11 ing in whole or in part in the capacity of—

12 (A) a health care provider, health benefit
13 plan, or health oversight agency; or

14 (B) an officer or employee of a person de-
15 scribed in subparagraph (A).

16 (7) PUBLIC HEALTH AUTHORITY.—The term
17 “public health authority” means an authority of the
18 United States, a State, or a political subdivision of
19 a State that—

20 (A) is responsible for public health mat-
21 ters; and

22 (B) is conducting—

23 (i) a disease or injury reporting pro-
24 gram;

25 (ii) public health surveillance; or

1 (iii) a public health investigation.

2 (8) PUBLIC HEALTH TRUSTEE.—The term
3 “public health trustee” means a person who, with
4 respect to protected health information, receives,
5 creates, uses, maintains, or transmits such informa-
6 tion while acting in whole or in part in the capacity
7 of—

8 (A) a health researcher;

9 (B) a public health authority; or

10 (C) an officer or employee of a person de-
11 scribed in subparagraph (A) or (B).

12 (9) SPECIAL PURPOSE TRUSTEE.—The term
13 “special purpose trustee” means a person who, with
14 respect to protected health information—

15 (A) receives such information under sec-
16 tion 126 (relating to emergency circumstances),
17 127 (relating to judicial, administrative, and
18 other legal purposes), 129 (relating to law en-
19 forcement), or 130 (relating to subpoenas, war-
20 rants, and search warrants); or

21 (B) is acting in whole or in part in the ca-
22 pacity of an officer or employee of a person de-
23 scribed in subparagraph (A) with respect to
24 such information.

25 (e) OTHER DEFINITIONS.—For purposes of this Act:

1 (1) **AFFILIATED PERSON.**—The term “affiliated
2 person” means a person who—

3 (A) is not a health information trustee;

4 (B) is a contractor, subcontractor, affiliate,
5 or subsidiary of a person who is a health infor-
6 mation trustee; and

7 (C) pursuant to an agreement or other re-
8 lationship with such trustee, receives, creates,
9 uses, maintains, or transmits protected health
10 information in order to conduct a legitimate
11 business activity of the trustee.

12 (2) **HEALTH CARE.**—The term “health care”—

13 (A) means—

14 (i) any preventive, diagnostic, thera-
15 peutic, rehabilitative, maintenance, or pal-
16 liative care, counseling, service, or
17 procedure—

18 (I) with respect to the physical or
19 mental condition of an individual; or

20 (II) affecting the structure or
21 function of the human body or any
22 part of the human body, including
23 banking of blood, sperm, organs, or
24 any other tissue; or

1 (ii) any sale or dispensing of a drug,
2 device, equipment, or other item to an indi-
3 vidual, or for the use of an individual, pur-
4 suant to a prescription; but

5 (B) does not include any item or service
6 that is not furnished for the purpose of main-
7 taining or improving the health of an individual.

8 (3) HEALTH RESEARCH PROJECT.—The term
9 “health research project” means a biomedical, epide-
10 miological, or health services research project, or a
11 health statistics project, that has been approved
12 by—

13 (A) an institutional review board for the
14 organization sponsoring the project;

15 (B) an institutional review board for each
16 health information trustee that maintains pro-
17 tected health information intended to be used in
18 the project; or

19 (C) an institutional review board estab-
20 lished or designated by the Secretary.

21 (4) INSTITUTIONAL REVIEW BOARD.—The term
22 “institutional review board” means—

23 (A) a board established in accordance with
24 regulations of the Secretary under section
25 491(a) of the Public Health Service Act;

1 (B) a similar board established by the Sec-
2 retary for the protection of human subjects in
3 research conducted by the Secretary;

4 (C) a similar board established under regu-
5 lations of a Federal Government authority other
6 than the Secretary; or

7 (D) a similar board which meets such re-
8 quirements as the Secretary may specify.

9 (5) LAW ENFORCEMENT INQUIRY.—The term
10 “law enforcement inquiry” means a lawful investiga-
11 tion or official proceeding inquiring into a specific
12 violation of, or failure to comply with, any criminal
13 or civil statute or any regulation, rule, or order is-
14 sued pursuant to such a statute.

15 (6) PERSON.—The term “person” includes an
16 authority of the United States, a State, or a political
17 subdivision of a State.

18 (7) SECRETARY.—The term “Secretary” means
19 the Secretary of Health and Human Services.

20 (8) STATE.—The term “State” includes the
21 District of Columbia, Puerto Rico, the Virgin Is-
22 lands, Guam, American Samoa, and the Northern
23 Mariana Islands.

1 **TITLE I—FAIR INFORMATION**
2 **PRACTICES FOR PROTECTED**
3 **HEALTH INFORMATION**

4 **Subtitle A—Treatment of Protected**
5 **Health Information**

6 **SEC. 101. DUTIES AND AUTHORITIES OF HEALTH USE**
7 **TRUSTEES.**

8 A health use trustee—

9 (1) shall comply with sections 111 (relating to
10 inspection), 112 (relating to amendment), 113 (re-
11 lating to notice of information practices), 114 (relat-
12 ing to accounting for disclosures), and 115 (relating
13 to security);

14 (2) may use protected health information if
15 such use is in accordance with section 121; and

16 (3) may disclose such information if such dis-
17 closure is in accordance with section 121 and 1 or
18 more of the following sections:

19 (A) Section 122 (relating to authoriza-
20 tions).

21 (B) Section 123 (relating to treatment,
22 payment, and oversight).

23 (C) Section 124 (relating to next of kin
24 and directory information).

25 (D) Section 125 (relating to public health).

1 (E) Section 126 (relating to emergency cir-
2 cumstances).

3 (F) Section 127 (relating to judicial, ad-
4 ministrative, and other legal purposes).

5 (G) Section 128 (relating to health re-
6 search).

7 (H) Section 129 (relating to law enforce-
8 ment).

9 (I) Section 130 (relating to subpoenas,
10 warrants, and search warrants).

11 **SEC. 102. DUTIES AND AUTHORITIES OF PUBLIC HEALTH**
12 **TRUSTEES.**

13 (a) IN GENERAL.—Except as provided in subsections
14 (b) and (c), a public health trustee—

15 (1) shall comply with sections 111 (relating to
16 inspection), 114 (relating to accounting for disclo-
17 sures), and 115 (relating to security);

18 (2) may use protected health information if
19 such use is in accordance with section 121; and

20 (3) may disclose such information if—

21 (A) such disclosure is essential to fulfill a
22 public health purpose; or

23 (B) such disclosure is in accordance with
24 section 121 and 1 or more of the following
25 sections:

1 (i) Section 122 (relating to authoriza-
2 tions).

3 (ii) Section 125 (relating to public
4 health).

5 (iii) Section 126 (relating to emer-
6 gency circumstances).

7 (iv) Section 128 (relating to health re-
8 search).

9 (v) Section 129 (relating to law en-
10 forcement) (except section 129(a)(2)).

11 (b) DETERMINATIONS BY PUBLIC HEALTH TRUST-
12 EES SPECIFIC TO AN INDIVIDUAL.—A public health trust-
13 ee who makes a decision concerning a right, benefit, or
14 privilege of a individual using protected health information
15 about the individual shall be considered to be a health use
16 trustee with respect to such information and is subject to
17 section 101 (and not this section) with respect to such
18 information.

19 (c) OVERLAP WITH HEALTH USE TRUSTEE.—A per-
20 son who is a public health trustee and a health use trustee
21 with respect to the same protected health information is
22 subject to section 101 and is not subject to this section
23 with respect to such information.

1 **SEC. 103. DUTIES AND AUTHORITIES OF SPECIAL PURPOSE**
2 **TRUSTEES.**

3 (a) IN GENERAL.—A special purpose trustee—

4 (1) shall comply with sections 114 (relating
5 to accounting for disclosures) and 115 (relating to
6 security);

7 (2) may use protected health information if
8 such use is in accordance with section 121; and

9 (3) may disclose such information if such dis-
10 closure is in accordance with section 121 and one or
11 more of the following sections:

12 (A) Section 122 (relating to authoriza-
13 tions).

14 (B) Section 126 (relating to emergency cir-
15 cumstances).

16 (C) Section 128 (relating to health re-
17 search).

18 (D) Section 129 (relating to law enforce-
19 ment).

20 (E) Section 130 (relating to subpoenas,
21 warrants, and search warrants).

22 (b) OVERLAP WITH HEALTH USE AND PUBLIC
23 HEALTH TRUSTEES.—A person who is a health use trust-
24 ee and a special purpose trustee with respect to the same
25 protected health information is subject to section 101 and
26 is not subject to this section with respect to such informa-

1 tion. A person who is a public health trustee and a special
2 purpose trustee with respect to the same protected health
3 information is subject to section 102 and is not subject
4 to this section with respect to such information.

5 **SEC. 104. DUTIES AND AUTHORITIES OF AFFILIATED PER-**
6 **SONS.**

7 (a) **DUTIES OF AFFILIATED PERSONS.—**

8 (1) **IN GENERAL.—**An affiliated person is re-
9 quired to fulfill any duty under this Act that—

10 (A) the health information trustee with
11 whom the person has an agreement or relation-
12 ship described in section 3(c)(1)(C) is required
13 to fulfill; and

14 (B) the person has undertaken to fulfill
15 pursuant to such agreement or relationship.

16 (2) **CONSTRUCTION OF OTHER SUBTITLES.—**

17 With respect to a duty described in paragraph (1)
18 that an affiliated person is required to fulfill, the
19 person shall be considered a health information
20 trustee for purposes of this Act. The person shall be
21 subject to subtitle E (relating to enforcement) with
22 respect to any such duty that the person fails to ful-
23 fill.

24 (3) **EFFECT ON TRUSTEE.—**An agreement or
25 relationship described in section 3(c)(1)(C) does not

1 relieve a health information trustee of any duty or
2 liability under this Act.

3 (b) AUTHORITIES.—

4 (1) IN GENERAL.—An affiliated person may ex-
5 ercise any authority under this Act that the health
6 information trustee with whom the person has an
7 agreement or relationship described in section
8 3(c)(1)(C) may exercise and that the person has
9 been given pursuant to such agreement. With re-
10 spect to any such authority, the person shall be con-
11 sidered a health information trustee for purposes of
12 this Act. The person shall be subject to subtitle E
13 (relating to enforcement) with respect to any act
14 that exceeds such authority.

15 (2) EFFECT ON TRUSTEE.—An agreement or
16 relationship described in section 3(c)(1)(C) does not
17 affect the authority of a health information trustee
18 under this Act.

1 **Subtitle B—Duties and Authorities**
2 **of Health Information Trustees**

3 **PART 1—DUTIES OF HEALTH INFORMATION**
4 **TRUSTEES**

5 **SEC. 111. INSPECTION OF PROTECTED HEALTH INFORMA-**
6 **TION.**

7 (a) **IN GENERAL.**—Except as provided in subsection
8 (b), a health information trustee who is required by sub-
9 title A to comply with this section—

10 (1) shall permit an individual to inspect any
11 protected health information about the individual
12 that the trustee maintains;

13 (2) shall permit the individual to have a copy
14 of the information;

15 (3) shall permit a person who has been des-
16 igned in writing by the individual to inspect, or to
17 have a copy of, the information on behalf of the indi-
18 vidual or to accompany the individual during the in-
19 spection; and

20 (4) may offer to explain or interpret informa-
21 tion that is inspected or copied under this sub-
22 section.

23 (b) **EXCEPTIONS.**—A health information trustee is
24 not required by this section to permit inspection or copy-

1 ing of protected health information if any of the following
2 conditions apply:

3 (1) MENTAL HEALTH TREATMENT NOTES.—

4 The information consists of psychiatric, psycholo-
5 gical, or mental health treatment notes, the trustee
6 determines in the exercise of reasonable medical
7 judgment that inspection or copying of the notes
8 would cause sufficient harm to the individual who is
9 the subject of the notes so as to outweigh the desir-
10 ability of permitting access, and the trustee does not
11 disclose the notes to any person not directly engaged
12 in treating the individual, except with the authoriza-
13 tion of the individual or under compulsion of law.

14 (2) INFORMATION ABOUT OTHERS.—The infor-

15 mation relates to an individual other than the indi-
16 vidual seeking to inspect or have a copy of the infor-
17 mation and the trustee determines in the exercise of
18 reasonable medical judgment that inspection or
19 copying of the information would cause sufficient
20 harm to one or both of the individuals so as to out-
21 weigh the desirability of permitting access.

22 (3) ENDANGERMENT TO LIFE OR SAFETY.—

23 Disclosure of the information could reasonably be
24 expected to endanger the life or physical safety of an
25 individual.

1 (4) CONFIDENTIAL SOURCE.—The information
2 identifies or could reasonably lead to the identifica-
3 tion of an individual (other than a health care pro-
4 vider) who provided information under a promise of
5 confidentiality to a health care provider concerning
6 the individual who is the subject of the information.

7 (5) ADMINISTRATIVE PURPOSES.—The
8 information—

9 (A) is used by the trustee solely for admin-
10 istrative purposes and not in the provision of
11 health care to the individual who is the subject
12 of the information; and

13 (B) is not disclosed by the trustee to any
14 person.

15 (6) DUPLICATIVE INFORMATION.—The informa-
16 tion duplicates information available for inspection
17 under subsection (a).

18 (7) INFORMATION COMPILED IN ANTICIPATION
19 OF LITIGATION.—The information is compiled
20 principally—

21 (A) in reasonable anticipation of a civil ac-
22 tion or proceeding; or

23 (B) for use in such an action or proceed-
24 ing.

1 (c) INSPECTION AND COPYING OF SEGREGABLE POR-
2 TION.—A health information trustee who is required by
3 subtitle A to comply with this section shall permit inspec-
4 tion and copying under subsection (a) of any reasonably
5 segregable portion of a record after deletion of any portion
6 that is exempt under subsection (b).

7 (d) CONDITIONS.—A health information trustee
8 may—

9 (1) require a written request for the inspection
10 and copying of protected health information under
11 this section; and

12 (2) charge a reasonable fee (not greater than
13 the actual cost) for—

14 (A) permitting inspection of information
15 under this section; and

16 (B) providing a copy of protected health
17 information under this section.

18 (e) STATEMENT OF REASONS FOR DENIAL.—If a
19 health information trustee denies a request for inspection
20 or copying under this section, the trustee shall provide the
21 individual who made the request (or the individual's des-
22 ignated representative) with a written statement of the
23 reasons for the denial.

24 (f) DEADLINE.—A health information trustee shall
25 comply with or deny a request for inspection or copying

1 of protected health information under this section within
2 the 30-day period beginning on the date the trustee re-
3 ceives the request.

4 **SEC. 112. AMENDMENT OF PROTECTED HEALTH INFORMA-**
5 **TION.**

6 (a) **IN GENERAL.**—A health information trustee who
7 is required by subtitle A to comply with this section shall,
8 within the 45-day period beginning on the date the trustee
9 receives from an individual about whom the trustee main-
10 tains protected health information a written request that
11 the trustee correct or amend the information, either—

12 (1) make the correction or amendment re-
13 quested, inform the individual of the correction or
14 amendment that has been made, and inform any
15 person who is identified by the individual, who is not
16 an employee of the trustee, and to whom the uncor-
17 rected or unamended portion of the information was
18 previously disclosed of the correction or amendment
19 that has been made; or

20 (2) inform the individual of—

21 (A) the reasons for the refusal of the trust-
22 ee to make the correction or amendment;

23 (B) any procedures for further review of
24 the refusal; and

1 (C) the individual's right to file with the
2 trustee a concise statement setting forth the re-
3 quested correction or amendment and the indi-
4 vidual's reasons for disagreeing with the refusal
5 of the trustee.

6 (b) BASES FOR REQUEST TO CORRECT OR AMEND.—
7 An individual may request correction or amendment of
8 protected health information about the individual under
9 subsection (a) if the information is not timely, accurate,
10 relevant, or complete.

11 (c) STATEMENT OF DISAGREEMENT.—After an indi-
12 vidual has filed a statement of disagreement under sub-
13 section (a)(2)(C), the trustee, in any subsequent disclosure
14 of the disputed portion of the information, shall include
15 a copy of the individual's statement and may include a
16 concise statement of the trustee's reasons for not making
17 the requested correction or amendment.

18 (d) CONSTRUCTION.—This section shall not be con-
19 strued to require a health information trustee to conduct
20 a formal, informal, or other hearing or proceeding con-
21 cerning a request for a correction or amendment to pro-
22 tected health information the trustee maintains.

23 (e) CORRECTION.—For purposes of subsection (a), a
24 correction is deemed to have been made to protected
25 health information where information that is not timely,

1 accurate, relevant, or complete is clearly marked as incor-
2 rect or where supplementary correct information is made
3 part of the information.

4 **SEC. 113. NOTICE OF INFORMATION PRACTICES.**

5 (a) **PREPARATION OF WRITTEN NOTICE.**—A health
6 information trustee who is required by subtitle A of this
7 title to comply with this section shall prepare a written
8 notice of information practices describing the following:

9 (1) **RIGHTS OF INDIVIDUALS.**—The rights
10 under this title of an individual who is the subject
11 of protected health information, including the right
12 to inspect and copy such information and the right
13 to seek amendments to such information, and the
14 procedures for authorizing disclosures of protected
15 health information and for revoking such authoriza-
16 tions.

17 (2) **PROCEDURES OF TRUSTEE.**—The proce-
18 dures established by the trustee for the exercise of
19 such rights.

20 (3) **AUTHORIZED DISCLOSURES.**—The dislo-
21 sures of protected health information that are au-
22 thorized under this Act.

23 (b) **DISSEMINATION OF NOTICE.**—A health informa-
24 tion trustee who is required by subtitle A to comply with
25 this section—

1 (1) shall, upon request, provide any person with
2 a copy of the trustee's notice of information prac-
3 tices (described in subsection (a)); and

4 (2) shall make reasonable efforts to inform per-
5 sons in a clear and conspicuous manner of the exist-
6 ence and availability of such notice.

7 (e) MODEL NOTICE.—Not later than July 1, 1996,
8 the Secretary, after notice and opportunity for public com-
9 ment, shall develop and disseminate a model notice of in-
10 formation practices for use by health information trustees
11 under this section.

12 **SEC. 114. ACCOUNTING FOR DISCLOSURES.**

13 (a) IN GENERAL.—A health information trustee who
14 is required by subtitle A to comply with this section shall
15 create and maintain, with respect to any protected health
16 information the trustee discloses, a record of—

17 (1) the date and purpose of the disclosure;

18 (2) the name of the person to whom the diselo-
19 sure was made;

20 (3) the address of the person to whom the dis-
21 closure was made or the location to which the diselo-
22 sure was made; and

23 (4) the information disclosed, but only where
24 the recording of the information disclosed is prac-
25 ticable, taking into account the technical capabilities

1 of the system used to maintain the record and the
2 costs of such maintenance.

3 (b) DISCLOSURE RECORD PART OF INFORMATION.—

4 A record created and maintained under subsection (a)
5 shall be maintained as part of the protected health infor-
6 mation to which the record pertains.

7 **SEC. 115. SECURITY.**

8 (a) IN GENERAL.—A health information trustee who
9 is required by subtitle A to comply with this section shall
10 maintain reasonable and appropriate administrative, tech-
11 nical, and physical safeguards—

12 (1) to ensure the integrity and confidentiality of
13 protected health information created or received by
14 the trustee;

15 (2) to protect against any anticipated threats or
16 hazards to the security or integrity of, improper dis-
17 closures of, or unauthorized uses of, such informa-
18 tion; and

19 (3) otherwise ensure compliance with this Act
20 by the trustee and the officers and employees of the
21 trustee.

22 (b) SPECIFIC SECURITY MEASURES.—A health infor-
23 mation trustee who is required by subtitle A to comply
24 with this section shall ensure that—

1 (1) officers, employees, and affiliated persons of
2 the trustee who have access to protected health in-
3 formation created or received by the trustee are reg-
4 ularly trained in the requirements governing such
5 information;

6 (2) audit trails are maintained, but only where
7 the maintenance of such trails is practicable, taking
8 into account the technical capabilities of the system
9 used to maintain protected health information and
10 the costs of such maintenance; and

11 (3) appropriate signs and warnings are posted
12 to advise persons described in paragraph (1) regard-
13 ing the need to secure protected health information.

14 **PART 2—USE AND DISCLOSURE OF PROTECTED**
15 **HEALTH INFORMATION**

16 **SEC. 121. GENERAL LIMITATIONS ON USE AND DISCLO-**
17 **SURE.**

18 (a) USE.—A health information trustee may use pro-
19 tected health information only for a purpose that is com-
20 patible with and related to the purpose for which the
21 information—

22 (1) was collected; or

23 (2) was received by the trustee.

1 (b) DISCLOSURE.—A health information trustee may
2 disclose protected health information only for a purpose
3 that is authorized under this Act.

4 (c) SCOPE OF USES AND DISCLOSURES.—

5 (1) IN GENERAL.—A use or disclosure of pro-
6 tected health information by a health information
7 trustee shall be limited, when practicable, to the
8 minimum amount of information necessary to ac-
9 complish the purpose for which the information is
10 used or disclosed.

11 (2) GUIDELINES.—Not later than July 1, 1996,
12 the Secretary, after notice and opportunity for pub-
13 lic comment, shall issue guidelines to implement
14 paragraph (1), which shall take into account the
15 technical capabilities of the record systems used to
16 maintain protected health information and the costs
17 of limiting use and disclosure.

18 (d) IDENTIFICATION OF DISCLOSED INFORMATION
19 AS PROTECTED INFORMATION.—Except with respect to
20 protected health information that is disclosed under sec-
21 tion 111 (relating to inspection) or 124 (relating to next
22 of kin and directory information), and except as provided
23 in subsection (e), a health information trustee may dis-
24 close protected health information only if such information

1 is clearly identified as protected health information that
2 is subject to this Act.

3 (e) ROUTINE DISCLOSURES SUBJECT TO WRITTEN
4 AGREEMENT.—A health information trustee who routinely
5 discloses protected health information to a person may
6 satisfy the identification requirement in subsection (d)
7 through the conclusion of a written agreement between the
8 trustee and the person with respect to the identification
9 of protected health information.

10 (f) AGREEMENT TO LIMIT USE OR DISCLOSURE.—
11 A health information trustee who receives protected health
12 information from any person pursuant to a written agree-
13 ment to restrict use or disclosure of the information to
14 a greater extent than would otherwise be required under
15 this Act shall comply with the terms of the agreement,
16 except where use or disclosure of the information in viola-
17 tion of the agreement is required by law. A trustee who
18 fails to comply with the preceding sentence shall be subject
19 to section 161 (relating to civil actions) with respect to
20 such failure.

21 (f) NO GENERAL REQUIREMENT TO DISCLOSE.—Ex-
22 cept as provided in section 111, nothing in this Act shall
23 be construed to require a health information trustee to dis-
24 close protected health information not otherwise required
25 to be disclosed by law.

1 **SEC. 122. AUTHORIZATIONS FOR DISCLOSURE OF PRO-**
2 **TECTED HEALTH INFORMATION.**

3 (a) **STATEMENT OF INTENDED USES AND DISCLO-**
4 **SURES.—**

5 (1) **IN GENERAL.**—A person who wishes to re-
6 ceive from a health information trustee protected
7 health information about an individual pursuant to
8 an authorization executed by the individual shall
9 supply the individual, in writing and on a form that
10 is distinct from the authorization, with a statement
11 of the uses for which the person intends the infor-
12 mation and the disclosures the person intends to
13 make of the information. Such statement shall be
14 supplied on or before the date on which the author-
15 ization is executed.

16 (2) **ENFORCEMENT.**—If the person uses or dis-
17 closes the information in a manner that is inconsis-
18 tent with such statement, the person shall be subject
19 to section 161 (relating to civil actions) with respect
20 to such failure, except where such use or disclosure
21 is required by law.

22 (3) **MODEL STATEMENTS.**—Not later than July
23 1, 1996, the Secretary, after notice and opportunity
24 for public comment, shall develop and disseminate
25 model statements of intended uses and disclosures of
26 the type described in paragraph (1).

1 (b) WRITTEN AUTHORIZATIONS.—A health informa-
2 tion trustee who is authorized by subtitle A to disclose
3 protected health information under this section may dis-
4 close such information pursuant to an authorization exe-
5 cuted by the individual who is the subject of the informa-
6 tion, if each of the following requirements is met:

7 (1) WRITING.—The authorization is in writing,
8 signed by the individual, and dated on the date of
9 such signature.

10 (2) SEPARATE FORM.—The authorization is not
11 on a form used to authorize or facilitate the provi-
12 sion of, or payment for, health care.

13 (3) TRUSTEE DESCRIBED.—The trustee is spe-
14 cifically named or generically described in the au-
15 thorization as authorized to disclose such informa-
16 tion.

17 (4) RECIPIENT DESCRIBED.—The person to
18 whom the information is to be disclosed is specifi-
19 cally named or generically described in the author-
20 ization as a person to whom such information may
21 be disclosed.

22 (5) STATEMENT OF INTENDED USES AND DIS-
23 CLOSURES RECEIVED.—The authorization contains
24 an acknowledgment that the individual has received

1 a statement described in subsection (a) from such
2 person.

3 (6) INFORMATION DESCRIBED.—The informa-
4 tion to be disclosed is described in the authorization.

5 (7) AUTHORIZATION TIMELY RECEIVED.—The
6 authorization is received by the trustee during a pe-
7 riod described in subsection (d)(1).

8 (8) DISCLOSURE TIMELY MADE.—The disclo-
9 sure occurs during a period described in subsection
10 (d)(2).

11 (c) AUTHORIZATIONS REQUESTED IN CONNECTION
12 WITH PROVISION OF HEALTH CARE.—

13 (1) IN GENERAL.—A health use trustee or a
14 public health trustee may not request that an indi-
15 vidual provide to any person an authorization de-
16 scribed in subsection (b) on a day on which—

17 (A) the trustee provides health care to the
18 individual; or

19 (B) in the case of a trustee that is a health
20 facility, the individual is admitted into the facil-
21 ity as a resident or inpatient in order to receive
22 health care.

23 (2) EXCEPTION.—Paragraph (1) does not apply
24 if a health use trustee or a public health trustee re-
25 quests that an individual provide an authorization

1 described in subsection (b) for the purpose of assist-
2 ing the individual in obtaining counseling or social
3 services from a person other than the trustee.

4 (d) TIME LIMITATIONS ON AUTHORIZATIONS.—

5 (1) RECEIPT BY TRUSTEE.—For purposes of
6 subsection (b)(7), an authorization is timely received
7 if it is received by the trustee during—

8 (A) the 1-year period beginning on the
9 date that the authorization is signed under sub-
10 section (b)(1), if the authorization permits the
11 disclosure of protected health information to a
12 health use trustee, public health trustee, or per-
13 son who provides counseling or social services to
14 individuals; or

15 (B) the 30-day period beginning on the
16 date that the authorization is signed under sub-
17 section (b)(1), if the authorization permits the
18 disclosure of protected health information to a
19 person other than a person described in sub-
20 paragraph (A).

21 (2) DISCLOSURE BY TRUSTEE.—For purposes
22 of subsection (b)(8), a disclosure is timely made if
23 it occurs before—

1 (A) the date or event (if any) specified in
2 the authorization upon which the authorization
3 expires; and

4 (B) the expiration of the 6-month period
5 beginning on the date the trustee receives the
6 authorization.

7 (e) REVOCATION OR AMENDMENT OF AUTHORIZA-
8 TION.—

9 (1) IN GENERAL.—An individual in writing may
10 revoke or amend an authorization described in sub-
11 section (b), in whole or in part, at any time, except
12 when—

13 (A) disclosure of protected health informa-
14 tion has been authorized to permit validation of
15 expenditures for health care, or based on health
16 condition, by a government authority; or

17 (B) action has been taken in reliance on
18 the authorization.

19 (2) NOTICE OF REVOCATION.—A health infor-
20 mation trustee who discloses protected health infor-
21 mation pursuant to an authorization that has been
22 revoked shall not be subject to any liability or pen-
23 alty under this Act if—

24 (A) the reliance was in good faith;

1 (B) the trustee had no notice of the rev-
2 ocation; and

3 (C) the disclosure was otherwise in accord-
4 ance with the requirements of this Act.

5 (f) EFFECT OF AUTHORIZATION ON PRIVILEGES.—

6 The execution by an individual of an authorization that
7 meets the requirements of this section for the purpose of
8 receiving health care or providing for the payment for
9 health care shall not be construed as affecting any privi-
10 lege that the individual may have under common or statu-
11 tory law in a court of a State or the United States.

12 (g) ADDITIONAL REQUIREMENTS OF TRUSTEE.—A
13 health information trustee may impose requirements for
14 an authorization that are in addition to the requirements
15 in this section.

16 (h) COPY.—A health information trustee who dis-
17 closes protected health information pursuant to an author-
18 ization under this section shall maintain a copy of the au-
19 thorization as part of the information.

20 (i) CONSTRUCTION.—This section shall not be
21 construed—

22 (1) to require a health information trustee to
23 disclose protected health information; or

1 (2) to limit the right of a health information
2 trustee to charge a fee for the disclosure or repro-
3 duction of protected health information.

4 (j) **SUBPOENAS, WARRANTS, AND SEARCH WAR-**
5 **RANTS.**—If a health information trustee discloses pro-
6 tected health information pursuant to an authorization in
7 order to comply with an administrative subpoena or war-
8 rant or a judicial subpoena or search warrant, the
9 authorization—

10 (1) shall specifically authorize the disclosure for
11 the purpose of permitting the trustee to comply with
12 the subpoena, warrant, or search warrant; and

13 (2) shall otherwise meet the requirements in
14 this section.

15 **SEC. 123. TREATMENT, PAYMENT, AND OVERSIGHT.**

16 (a) **IN GENERAL.**—A health information trustee who
17 is authorized by subtitle A to disclose protected health in-
18 formation under this section may disclose such informa-
19 tion to a health use trustee if the disclosure is—

20 (1) for the purpose of providing health care to
21 an individual and the individual who is the subject
22 of the information has not previously objected to the
23 disclosure in writing;

24 (2) for the purpose of providing for the pay-
25 ment for health care furnished to an individual; or

1 (3) for use by a health oversight agency for a
2 purpose authorized by law.

3 (b) USE IN ACTION AGAINST INDIVIDUAL.—Pro-
4 tected health information about an individual that is dis-
5 closed under this section may not be used in, or disclosed
6 to any person for use in, any administrative, civil, or erimi-
7 nal action or investigation directed against the individual,
8 except an action or investigation arising out of and di-
9 rectly related to receipt of health care or payment for
10 health care. ‘

11 **SEC. 124. NEXT OF KIN AND DIRECTORY INFORMATION.**

12 (a) NEXT OF KIN.—A health information trustee who
13 is authorized by subtitle A to disclose protected health in-
14 formation under this section may disclose such informa-
15 tion to the next of kin or legal representative (as defined
16 under State law) of the individual who is the subject of
17 the information, or to a person with whom the individual
18 has a personal relationship, if—

19 (1) the individual has not previously objected to
20 the disclosure;

21 (2) the disclosure is consistent with accepted
22 medical practice; and

23 (3) the information disclosed relates to the on-
24 going provision of health care to the individual.

1 (b) DIRECTORY INFORMATION.—A health informa-
2 tion trustee who is authorized by subtitle A to disclose
3 protected health information under this section may dis-
4 close such information to any person, if—

5 (1) the information does not reveal specific in-
6 formation about the physical or mental condition of
7 the individual or health care provided to the individ-
8 ual;

9 (2) the individual who is the subject of the in-
10 formation has not objected in writing to the disclo-
11 sure;

12 (3) the disclosure is consistent with accepted
13 medical practice; and

14 (4) the information consists only of 1 or more
15 of the following items:

16 (A) The name of the individual.

17 (B) If the individual is receiving health
18 care from a health care provider on a premises
19 controlled by the provider, the location of the
20 individual on such premises.

21 (C) If the individual is receiving health
22 care from a health care provider on a premises
23 controlled by the provider, the general health
24 status of the individual, described in terms of

1 critical, poor, fair, stable, satisfactory, or terms
2 denoting similar conditions.

3 (c) RECIPIENTS.—A person to whom protected health
4 information is disclosed under this section shall not, by
5 reason of such disclosure, be subject to any requirement
6 under this Act.

7 **SEC. 125. PUBLIC HEALTH.**

8 (a) IN GENERAL.—A health information trustee who
9 is authorized by subtitle A to disclose protected health in-
10 formation under this section may disclose such informa-
11 tion to a public health trustee for use in legally
12 authorized—

- 13 (1) disease or injury reporting;
14 (2) public health surveillance; or
15 (3) public health investigation.

16 (b) USE IN ACTION AGAINST INDIVIDUAL.—Pro-
17 tected health information about an individual that is dis-
18 closed under this section may not be used in, or disclosed
19 to any person for use in, any administrative, civil, or crimi-
20 nal action or investigation directed against the individual,
21 except where the use or disclosure is authorized by law
22 for protection of the public health.

23 **SEC. 126. EMERGENCY CIRCUMSTANCES.**

24 A health information trustee who is authorized by
25 subtitle A to disclose protected health information under

1 this section may disclose such information to alleviate
2 emergency circumstances affecting the health or safety of
3 an individual.

4 **SEC. 127. JUDICIAL, ADMINISTRATIVE, AND OTHER LEGAL**
5 **PURPOSES.**

6 (a) **IN GENERAL.**—A health information trustee who
7 is authorized by subtitle A to disclose protected health in-
8 formation under this section may disclose such
9 information—

10 (1) pursuant to the Federal Rules of Civil Pro-
11 cedure, the Federal Rules of Criminal Procedure, or
12 comparable rules of other courts or administrative
13 agencies in connection with litigation or proceedings
14 to which the individual who is the subject of the in-
15 formation is a party and in which the individual has
16 placed the individual's physical or mental condition
17 in issue;

18 (2) pursuant to a law requiring the reporting of
19 specific medical information to law enforcement au-
20 thorities;

21 (3) if the disclosure is of information described
22 in paragraph (2) and the trustee is operated by a
23 Federal agency;

24 (4) if directed by a court in connection with a
25 court-ordered examination of an individual; or

1 (5) to assist in the identification of a dead indi-
2 vidual.

3 (b) WRITTEN STATEMENT.—A person seeking pro-
4 tected health information about an individual maintained
5 by health information trustee under—

6 (1) subsection (a)(1) shall provide the trustee
7 with a written statement that the individual is a
8 party to the litigation or proceedings for which the
9 information is sought; or

10 (2) subsection (a)(5) shall provide the trustee
11 with a written statement that the information is
12 sought to assist in the identification of a dead indi-
13 vidual.

14 (c) USE AND DISCLOSURE.—A person to whom pro-
15 tected health information is disclosed under this section
16 may use and disclose the information only under a condi-
17 tion described in subsection (a).

18 **SEC. 128. HEALTH RESEARCH.**

19 (a) IN GENERAL.—A health information trustee who
20 is authorized by subtitle A to disclose protected health in-
21 formation under this section may disclose such informa-
22 tion to a public health trustee if the disclosure is for use
23 in a health research project that has been determined by
24 an institutional review board to be—

1 (1) of sufficient importance so as to outweigh
2 the intrusion into the privacy of the individual who
3 is the subject of the information that would result
4 from the disclosure; and

5 (2) reasonably impracticable to conduct without
6 such information.

7 (b) OBLIGATIONS OF RECIPIENT.—A person who re-
8 ceives protected health information pursuant to subsection
9 (a) shall remove or destroy, at the earliest opportunity
10 consistent with the purposes of the project, information
11 that would enable 1 or more individuals to be identified,
12 unless an institutional review board has determined that
13 there is a health or research justification for retention of
14 such identifiers and there is an adequate plan to protect
15 the identifiers from use and disclosure that is inconsistent
16 with this Act.

17 **SEC. 129. LAW ENFORCEMENT.**

18 (a) IN GENERAL.—A health information trustee who
19 is authorized by subtitle A to disclose protected health in-
20 formation under this section may disclose such informa-
21 tion to a law enforcement agency (other than a health
22 oversight agency) if the information is—

23 (1) for use in an investigation or prosecution of
24 a health information trustee;

1 (2) to assist in the identification or location of
2 a suspect, fugitive, or witness in a law enforcement
3 inquiry;

4 (3) in connection with criminal activity commit-
5 ted against the trustee or an affiliated person of the
6 trustee or on premises controlled by the trustee; or

7 (4) needed to determine whether a crime has
8 been committed and the nature of any crime that
9 may have been committed (other than a crime that
10 may have been committed by the individual who is
11 the subject of the information).

12 (b) CERTIFICATION.—Where a law enforcement
13 agency requests a health information trustee to disclose
14 protected health information under this section, the agen-
15 cy shall provide the trustee with a written certification
16 that—

17 (1) is signed by a supervisory official of a rank
18 designated by the head of the agency;

19 (2) specifies the information requested; and

20 (3) states that the information is needed for a
21 lawful purpose under this section.

22 (c) RESTRICTIONS ON DISCLOSURE AND USE.—Pro-
23 tected health information about an individual that is dis-
24 closed by a health information trustee to a law enforce-
25 ment agency under this section—

1 (1) may not be disclosed for, or used in, any
2 administrative, civil, or criminal action or investiga-
3 tion against the individual, except in an action or in-
4 vestigation arising out of and directly related to the
5 action or investigation for which the information was
6 obtained; and

7 (2) may not be otherwise used or disclosed by
8 the agency, unless the use or disclosure is necessary
9 to fulfill the purpose for which the information was
10 obtained and is not otherwise prohibited by law.

11 **SEC. 130. SUBPOENAS, WARRANTS, AND SEARCH WAR-**
12 **RANTS.**

13 (a) **IN GENERAL.**—A health information trustee who
14 is authorized by subtitle A to disclose protected health in-
15 formation under this section may disclose such informa-
16 tion if the disclosure is pursuant to any of the following:

17 (1) A subpoena issued under the authority of a
18 grand jury and the trustee is provided a written cer-
19 tification by the grand jury seeking the information
20 that the grand jury has complied with the applicable
21 access provisions of section 141 or 143(a).

22 (2) An administrative subpoena or warrant or
23 a judicial subpoena or search warrant and the trust-
24 ee is provided a written certification by the person
25 seeking the information that the person has com-

1 plied with the applicable access provisions of section
2 141 or 143(a).

3 (3) An administrative subpoena or warrant or
4 a judicial subpoena or search warrant and the dis-
5 closure otherwise meets the conditions of one of sec-
6 tions 123 through 129.

7 (b) RESTRICTIONS ON USE AND DISCLOSURE.—Pro-
8 tected health information about an individual that is dis-
9 closed by a health information trustee under—

10 (1) subsection (a) may not be disclosed for, or
11 used in, any administrative, civil, or criminal action
12 or investigation against the individual, except in an
13 action or investigation arising out of and directly re-
14 lated to the inquiry for which the information was
15 obtained;

16 (2) subsection (a)(2) may not be otherwise used
17 or disclosed by the recipient unless the use or disclo-
18 sure is necessary to fulfill the purpose for which the
19 information was obtained; and

20 (3) subsection (a)(3) may not be used or dis-
21 closed by the recipient unless the recipient complies
22 with the conditions and restrictions on use and dis-
23 closure with which the recipient would have been re-
24 quired to comply if the disclosure by the trustee had
25 been made under the section referred to in sub-

1 section (a)(3) the conditions of which were met by
2 the disclosure.

3 (e) RESTRICTIONS ON GRAND JURIES.—Protected
4 health information that is disclosed by a health informa-
5 tion trustee under subsection (a)(1)—

6 (1) shall be returnable on a date when the
7 grand jury is in session and actually presented to
8 the grand jury;

9 (2) shall be used only for the purpose of consid-
10 ering whether to issue an indictment or report by
11 that grand jury, or for the purpose of prosecuting a
12 crime for which that indictment or report is issued,
13 or for a purpose authorized by rule 6(e) of the Fed-
14 eral Rules of Criminal Procedure or a comparable
15 State rule;

16 (3) shall be destroyed or returned to the trustee
17 if not used for one of the purposes specified in para-
18 graph (2); and

19 (4) shall not be maintained, or a description of
20 the contents of such information shall not be main-
21 tained, by any government authority other than in
22 the sealed records of the grand jury, unless such in-
23 formation has been used in the prosecution of a
24 crime for which the grand jury issued an indictment
25 or presentment or for a purpose authorized by rule

1 6(e) of the Federal Rules of Criminal Procedure or
2 a comparable State rule.

3 (d) COPY AS PART OF PROTECTED INFORMATION.—
4 A health information trustee who discloses protected
5 health information under this section shall maintain a
6 copy of the applicable subpoena, warrant, or search war-
7 rant as part of the information.

8 (e) CONSTRUCTION.—Nothing in this section shall be
9 construed as authority for a health information trustee to
10 refuse to comply with an administrative subpoena or war-
11 rant or a judicial subpoena or search warrant that meets
12 the requirements of this Act.

13 **Subtitle C—Access Procedures and** 14 **Challenge Rights**

15 **SEC. 141. ACCESS PROCEDURES FOR LAW ENFORCEMENT** 16 **SUBPOENAS, WARRANTS, AND SEARCH WAR-** 17 **RANTS.**

18 (a) PROBABLE CAUSE REQUIREMENT.—A govern-
19 ment authority may not obtain protected health informa-
20 tion about an individual from a health information trustee
21 under paragraph (1) or (2) of section 130(a) for use in
22 a law enforcement inquiry unless there is probable cause
23 to believe that the information is relevant to a legitimate
24 law enforcement inquiry being conducted by the govern-
25 ment authority.

1 (b) WARRANTS AND SEARCH WARRANTS.—A govern-
2 ment authority that obtains protected health information
3 about an individual from a health information trustee
4 under circumstances described in subsection (a) and pur-
5 suant to a warrant or search warrant shall, not later than
6 30 days after the date the warrant was served on the
7 trustee, serve the individual with, or mail to the last
8 known address of the individual, a copy of the warrant.

9 (c) SUBPOENAS.—Except as provided in subsection
10 (d), a government authority may not obtain protected
11 health information about an individual from a health in-
12 formation trustee under circumstances described in sub-
13 section (a) and pursuant to a subpoena unless a copy of
14 the subpoena has been served by hand delivery upon the
15 individual, or mailed to the last known address of the indi-
16 vidual, on or before the date on which the subpoena was
17 served on the trustee, together with a notice (published
18 by the Secretary under section 145(1)) of the individual's
19 right to challenge the subpoena in accordance with section
20 142, and—

21 (1) 30 days have passed from the date of serv-
22 ice, or 30 days have passed from the date of mailing,
23 and within such time period the individual has not
24 initiated a challenge in accordance with section 142;
25 or

1 (2) disclosure is ordered by a court under sec-
2 tion 142.

3 (d) APPLICATION FOR DELAY.—

4 (1) IN GENERAL.—A government authority may
5 apply to an appropriate court to delay (for an initial
6 period of not longer than 90 days) serving a copy of
7 a subpoena and a notice otherwise required under
8 subsection (c) with respect to a law enforcement in-
9 quiry. The government authority may apply to the
10 court for extensions of the delay.

11 (2) REASONS FOR DELAY.—An application for
12 a delay, or extension of a delay, under this sub-
13 section shall state, with reasonable specificity, the
14 reasons why the delay or extension is being sought.

15 (3) EX PARTE ORDER.—The court shall enter
16 an ex parte order delaying, or extending the delay
17 of, the notice and an order prohibiting the trustee
18 from revealing the request for, or the disclosure of,
19 the protected health information being sought if the
20 court finds that—

21 (A) the inquiry being conducted is within
22 the lawful jurisdiction of the government au-
23 thority seeking the protected health informa-
24 tion;

1 (B) there is probable cause to believe that
2 the protected health information being sought is
3 relevant to a legitimate law enforcement inquiry
4 being conducted by the government authority;

5 (C) the government authority's need for
6 the information outweighs the privacy interest
7 of the individual who is the subject of the infor-
8 mation; and

9 (D) there are reasonable grounds to believe
10 that receipt of a notice by the individual will re-
11 sult in—

12 (i) endangering the life or physical
13 safety of any individual;

14 (ii) flight from prosecution;

15 (iii) destruction of or tampering with
16 evidence or the information being sought;
17 or

18 (iv) intimidation of potential wit-
19 nesses.

20 (4) SERVICE OF APPLICATION ON INDIVID-
21 UAL.—Upon the expiration of a period of delay of
22 notice under this subsection, the government author-
23 ity shall serve upon the individual, with the service
24 of the subpoena and the notice, a copy of any appli-
25 cations filed and approved under this subsection.

1 **SEC. 142. CHALLENGE PROCEDURES FOR LAW ENFORCE-**
2 **MENT SUBPOENAS.**

3 (a) **MOTION TO QUASH SUBPOENA.**—Within 30 days
4 of the date of service, or 30 days of the date of mailing,
5 of a subpoena of a government authority seeking protected
6 health information about an individual from a health in-
7 formation trustee under paragraph (1) or (2) of section
8 130(a) (except a subpoena issued in compliance with the
9 provisions of section 143(a)), the individual may file (with-
10 out filing fee) a motion to quash the subpoena—

11 (1) in the case of a State judicial subpoena, in
12 the court which issued the subpoena;

13 (2) in the case of a subpoena issued under the
14 authority of a State that is not a State judicial sub-
15 poena, in a court of competent jurisdiction;

16 (3) in the case of a subpoena issued under the
17 authority of a Federal court, in any court of the
18 United States of competent jurisdiction; or

19 (4) in the case of any other subpoena issued
20 under the authority of the United States, in—

21 (A) the United States district court for the
22 district in which the individual resides or in
23 which the subpoena was issued; or

24 (B) another United States district court of
25 competent jurisdiction.

1 (b) COPY.—A copy of the motion shall be served by
2 the individual upon the government authority by delivery
3 of registered or certified mail.

4 (c) AFFIDAVITS AND SWORN DOCUMENTS.—The gov-
5 ernment authority may file with the court such affidavits
6 and other sworn documents as sustain the validity of the
7 subpoena. The individual may file with the court, within
8 5 days of the date of the authority's filing, affidavits and
9 sworn documents in response to the authority's filing. The
10 court, upon the request of the individual, the government
11 authority, or both, may proceed in camera.

12 (d) PROCEEDINGS AND DECISION ON MOTION.—The
13 court may conduct such proceedings as it deems appro-
14 priate to rule on the motion. All such proceedings shall
15 be completed, and the motion ruled on, within 10 calendar
16 days of the date of the government authority's filing.

17 (e) EXTENSION OF TIME LIMITS FOR GOOD
18 CAUSE.—The court, for good cause shown, may at any
19 time in its discretion enlarge the time limits established
20 by subsections (c) and (d).

21 (f) STANDARD FOR DECISION.—A court may deny an
22 individual's timely motion under subsection (a) if it finds
23 that there is probable cause to believe that the protected
24 health information being sought is relevant to a legitimate
25 law enforcement inquiry being conducted by the govern-

1 ment authority, unless the court finds that the individual's
2 privacy interest outweighs the government authority's
3 need for the information. The individual shall have the
4 burden of demonstrating that the individual's privacy in-
5 terest outweighs the need established by the government
6 authority for the information.

7 (g) SPECIFIC CONSIDERATIONS WITH RESPECT TO
8 PRIVACY INTEREST.—In determining under subsection (f)
9 whether an individual's privacy interest outweighs the gov-
10 ernment authority's need for the information, the court
11 shall consider—

12 (1) the particular purpose for which the infor-
13 mation was collected by the trustee;

14 (2) the degree to which disclosure of the infor-
15 mation will embarrass, injure, or invade the privacy
16 of the individual;

17 (3) the effect of the disclosure on the individ-
18 ual's future health care;

19 (4) the importance of the inquiry being con-
20 ducted by the government authority, and the impor-
21 tance of the information to that inquiry; and

22 (5) any other factor deemed relevant by the
23 court.

24 (h) ATTORNEY'S FEES.—In the case of any motion
25 brought under subsection (a) in which the individual has

1 substantially prevailed, the court, in its discretion, may as-
2 sess against a government authority a reasonable attor-
3 ney's fee and other litigation costs (including expert fees)
4 reasonably incurred.

5 (i) NO INTERLOCUTORY APPEAL.—A court ruling de-
6 nying a motion to quash under this section shall not be
7 deemed a final order and no interlocutory appeal may be
8 taken therefrom by the individual. An appeal of such a
9 ruling may be taken by the individual within such period
10 of time as is provided by law as part of any appeal from
11 a final order in any legal proceeding initiated against the
12 individual arising out of or based upon the protect health
13 information disclosed.

14 **SEC. 143. ACCESS AND CHALLENGE PROCEDURES FOR**
15 **OTHER SUBPOENAS.**

16 (a) IN GENERAL.—A person (other than a govern-
17 ment authority under section 141) may not obtain pro-
18 tected health information about an individual from a
19 health information trustee pursuant to a subpoena under
20 section 130(a)(2) unless—

21 (1) a copy of the subpoena has been served
22 upon the individual or mailed to the last known ad-
23 dress of the individual on or before the date on
24 which the subpoena was served on the trustee, to-
25 gether with a notice (published by the Secretary

1 under section 145(2)) of the individual's right to
2 challenge the subpoena, in accordance with sub-
3 section (b); and

4 (2) either—

5 (A) 30 days have passed from the date of
6 service or 30 days have passed from the date of
7 the mailing and within such time period the in-
8 dividual has not initiated a challenge in accord-
9 ance with subsection (b); or

10 (B) disclosure is ordered by a court under
11 such subsection.

12 (b) MOTION TO QUASH.—Within 30 days of the date
13 of service or 30 days of the date of mailing of a subpoena
14 seeking protected health information about an individual
15 from a health information trustee under subsection (a),
16 the individual may file (without filing fee) in any court
17 of competent jurisdiction, a motion to quash the subpoena,
18 with a copy served on the person seeking the information.
19 The individual may oppose, or seek to limit, the subpoena
20 on any grounds that would otherwise be available if the
21 individual were in possession of the information.

22 (c) STANDARD FOR DECISION.—The court shall
23 grant an individual's timely motion under subsection (b)
24 if the person seeking the information has not sustained
25 the burden of demonstrating that—

1 (1) there are reasonable grounds to believe that
2 the information will be relevant to a lawsuit or other
3 judicial or administrative proceeding; and

4 (2) the need of the person for the information
5 outweighs the privacy interest of the individual.

6 (d) SPECIFIC CONSIDERATIONS WITH RESPECT TO
7 PRIVACY INTEREST.—In determining under subsection (c)
8 whether the need of the person for the information out-
9 weighs the privacy interest of the individual, the court
10 shall consider—

11 (1) the particular purpose for which the infor-
12 mation was collected by the trustee;

13 (2) the degree to which disclosure of the infor-
14 mation will embarrass, injure, or invade the privacy
15 of the individual;

16 (3) the effect of the disclosure on the individ-
17 ual's future health care;

18 (4) the importance of the information to the
19 lawsuit or proceeding; and

20 (5) any other factor deemed relevant by the
21 court.

22 (e) ATTORNEY'S FEES.—In the case of any motion
23 brought under subsection (b) by an individual against a
24 person in which the individual has substantially prevailed,
25 the court, in its discretion, may assess against the person

1 a reasonable attorney's fee and other litigation costs (in-
2 cluding expert fees) reasonably incurred.

3 **SEC. 144. CONSTRUCTION OF SUBTITLE; SUSPENSION OF**
4 **STATUTE OF LIMITATIONS.**

5 (a) IN GENERAL.—Nothing in this subtitle shall af-
6 fect the right of a health information trustee to challenge
7 requests for protected health information. Nothing in this
8 subtitle shall entitle an individual who is the subject of
9 such information to assert the rights of a health informa-
10 tion trustee.

11 (b) EFFECT OF MOTION ON STATUTE OF LIMITA-
12 TIONS.—If an individual who is the subject of protected
13 health information files a motion under this Act which has
14 the effect of delaying the access of a government authority
15 to such information, any applicable statute of limitations
16 is deemed to be tolled for the period beginning on the date
17 such motion was filed and ending on the date on which
18 the motion is decided.

19 **SEC. 145. RESPONSIBILITIES OF SECRETARY.**

20 Not later than July 1, 1996, the Secretary, after no-
21 tice and opportunity for public comment, shall develop and
22 disseminate a brief, clear, and easily understood notice—

23 (1) for use under subsection (c) of section 141,
24 detailing the rights of an individual who wishes to
25 challenge, under section 142, the disclosure of pro-

1 tected health information about the individual under
2 such subsection; and

3 (2) for use under subsection (a) of section 143,
4 detailing the rights of an individual who wishes to
5 challenge, under subsection (b) of such section, the
6 disclosure of protected health information about the
7 individual under such section.

8 **Subtitle D—Miscellaneous** 9 **Provisions**

10 **SEC. 151. DEBIT AND CREDIT CARD TRANSACTIONS.**

11 (a) **PAYMENT FOR HEALTH CARE THROUGH DEBIT**
12 **OR CREDIT CARD.**—If an individual pays a health infor-
13 mation trustee for health care by presenting a debit or
14 credit card or card number, the trustee may use or dis-
15 close such protected health information about the individ-
16 ual as is necessary for the processing of the debit or credit
17 card transaction or the billing or collection of amounts
18 charged or debited to the individual using the card or
19 number.

20 (b) **TRANSACTION PROCESSING BY CARD ISSUERS.**—
21 A person who is a debit or credit card issuer or is other-
22 wise directly involved in the processing of credit or debit
23 transactions or the billing or collection of amounts charged
24 or debited thereto may only use or disclose protected
25 health information about an individual—

1 (1) that has been disclosed in accordance with
2 subsection (a); and

3 (2) when necessary for—

4 (A) the billing or collection of amounts
5 charged or debited to the individual using a
6 debit or credit card;

7 (B) the transfer of receivables, accounts,
8 or interest therein;

9 (C) the audit of the credit or debit card ac-
10 count information;

11 (D) compliance with Federal, State, or
12 local law; and

13 (E) a properly authorized civil, criminal, or
14 regulatory investigation by Federal, State, or
15 local authorities.

16 **SEC. 152. ACCESS TO PROTECTED HEALTH INFORMATION**
17 **OUTSIDE OF THE UNITED STATES.**

18 (a) **IN GENERAL.**—Except as provided in subsection
19 (b), notwithstanding the provisions of subtitle A and part
20 2 of subtitle B, a health information trustee may not per-
21 mit any person who is not in a State to have access to
22 protected health information about an individual unless
23 one or more of the following conditions exist:

24 (1) **SPECIFIC AUTHORIZATION.**—The individual
25 has specifically consented to the provision of such

1 access outside of the United States in an authoriza-
2 tion that meets the requirements of section 122.

3 (2) EQUIVALENT INFORMATION PRACTICES.—

4 The provision of such access is authorized under this
5 Act and the Secretary has determined that there are
6 fair information practices for protected health infor-
7 mation in the country where the access will be pro-
8 vided that are equivalent to the fair information
9 practices provided for by this Act.

10 (3) ACCESS REQUIRED BY LAW.—The provision
11 of such access is required under—

12 (A) a Federal statute; or

13 (B) a treaty or other international agree-
14 ment applicable to the United States.

15 (b) EXCEPTIONS.—Subsection (a) does not apply
16 where the provision of access to protected health
17 information—

18 (1) is to a foreign public health authority;

19 (2) is authorized under section 126; or

20 (3) is necessary for the purpose of providing for
21 payment for health care that has been provided to
22 an individual.

1 **SEC. 153. STANDARDS FOR ELECTRONIC DOCUMENTS AND**
2 **COMMUNICATIONS.**

3 (a) **STANDARDS.**—Not later than July 1, 1996, the
4 Secretary, after notice and opportunity for public com-
5 ment, shall promulgate standards with respect to the cre-
6 ation, transmission, receipt, and maintenance, in elec-
7 tronic form, of each written document required or author-
8 ized under this Act. Where a signature is required with
9 respect to a written document under any other provision
10 of this Act, such standards shall provide for an electronic
11 substitute that serves the functional equivalent of a
12 signature.

13 (b) **TREATMENT OF COMPLYING DOCUMENTS AND**
14 **COMMUNICATIONS.**—An electronic document or commu-
15 nication that satisfies the standards promulgated under
16 subsection (a) with respect to such document or commu-
17 nication shall be treated as satisfying the requirements of
18 this Act that apply to an equivalent written document.

19 **SEC. 154. POWERS OF ATTORNEY.**

20 In the case of an individual who has executed a power
21 of attorney, recognized under State law, authorizing a per-
22 son to act as agent or attorney for the individual for one
23 or more purposes, the person may exercise any right of
24 the individual under this title that the person is authorized
25 to exercise by the power of attorney, if—

1 (1) any condition precedent to the exercise of
2 such right that is set forth in the power of attorney
3 has been satisfied; and

4 (2) the power of attorney specifically referenees
5 or describes the rights under this title that may be
6 exercised by the person.

7 **SEC. 155. RIGHTS OF INCOMPETENTS.**

8 (a) **EFFECT OF DECLARATION OF INCOMPETENCE.—**

9 Except as provided in section 154, if an individual has
10 been declared to be incompetent by a court of competent
11 jurisdiction, the rights of the individual under this title
12 shall be exercised and discharged in the best interests of
13 the individual through an authorized legal representative
14 of the individual.

15 (b) **NO COURT DECLARATION.—**Except as provided
16 in section 154, if a health care provider determines that
17 an individual, who has not been declared to be incom-
18 petent by a court of competent jurisdiction, suffers from
19 a medical condition that prevents the individual from act-
20 ing knowingly or effectively on the individual's own behalf,
21 the right of the individual to authorize disclosure under
22 section 122 may be exercised and discharged in the best
23 interest of the individual by the individual's next of kin.

1 **SEC. 156. RIGHTS OF MINORS.**

2 (a) INDIVIDUALS WHO ARE 18 OR LEGALLY CAPA-
3 BLE.—In the case of an individual—

4 (1) who is 18 years of age or older, all rights
5 of the individual shall be exercised by the individual,
6 except as provided in sections 154 and 155; or

7 (2) who, acting alone, has the legal capacity to
8 apply for and obtain a type of medical examination,
9 care, or treatment and who has sought such exam-
10 ination, care, or treatment, the individual shall exer-
11 cise all rights of an individual under this title with
12 respect to protected health information relating to
13 such examination, care, or treatment.

14 (b) INDIVIDUALS UNDER 18.—Except as provided in
15 subsection (a)(2), in the case of an individual who is—

16 (1) under 14 years of age, all the individual's
17 rights under this title shall be exercised through the
18 parent or legal guardian of the individual; or

19 (2) 14, 15, 16, or 17 years of age, the right of
20 inspection (under section 111), the right of amend-
21 ment (under section 112), and the right to authorize
22 disclosure of protected health information (under
23 section 122) of the individual may be exercised ei-
24 ther by the individual or by the parent or legal
25 guardian of the individual.

1 **Subtitle E—Enforcement**

2 **SEC. 161. CIVIL ACTIONS.**

3 (a) **IN GENERAL.**—Any individual whose rights under
4 this title have been knowingly or negligently violated—

5 (1) by a health information trustee, or any
6 other person, who is not described in paragraph (2),
7 (3), (4), or (5) may maintain a civil action for actual
8 damages and for equitable relief against the health
9 information trustee or other person;

10 (2) by an officer or employee of the United
11 States while the officer or employee was acting with-
12 in the scope of the office or employment may main-
13 tain a civil action for actual damages and for equi-
14 table relief against the United States;

15 (3) by an officer or employee of any government
16 authority of a State that has waived its sovereign
17 immunity to a claim for damages resulting from a
18 violation of this title while the officer or employee
19 was acting within the scope of the office or employ-
20 ment may maintain a civil action for actual damages
21 and for equitable relief against the State govern-
22 ment;

23 (4) by an officer or employee of a government
24 of a State that is not described in paragraph (3)
25 may maintain a civil action for actual damages and

1 for equitable relief against the officer or employee;
2 or

3 (5) by an officer or employee of a government
4 authority while the officer or employee was not act-
5 ing within the scope of the office or employment
6 may maintain a civil action for actual damages and
7 for equitable relief against the officer or employee.

8 (b) KNOWING VIOLATIONS.—Any individual entitled
9 to recover actual damages under this section because of
10 a knowing violation of a provision of this title (other than
11 subsection (c) or (d) of section 121) shall be entitled to
12 recover the amount of the actual damages demonstrated
13 or \$5000, whichever is greater.

14 (c) ACTUAL DAMAGES.—For purposes of this section,
15 the term “actual damages” includes damages paid to com-
16 pensate an individual for nonpecuniary losses such as
17 physical and mental injury as well as damages paid to
18 compensate for pecuniary losses.

19 (d) PUNITIVE DAMAGES; ATTORNEY’S FEES.—In
20 any action brought under this section in which the com-
21 plainant has prevailed because of a knowing violation of
22 a provision of this title (other than subsection (c) or (d)
23 of section 121), the court may, in addition to any relief
24 awarded under subsections (a) and (b), award such puni-
25 tive damages as may be warranted. In such an action, the

1 court, in its discretion, may allow the prevailing party a
2 reasonable attorney's fee (including expert fees) as part
3 of the costs, and the United States shall be liable for costs
4 the same as a private person.

5 (e) INSPECTION AND AMENDMENT.—If a health in-
6 formation trustee has established a written internal proce-
7 dure that allows an individual who has been denied inspec-
8 tion or amendment of protected health information to ap-
9 peal the denial, the individual may not maintain a civil
10 action in connection with the denial until the earlier of—

11 (1) the date the appeal procedure has been ex-
12 hausted; or

13 (2) 3 months after the date the original request
14 for inspection or amendment was made.

15 (f) NO LIABILITY FOR PERMISSIBLE DISCLO-
16 SURES.—A health information trustee who makes a disclo-
17 sure of protected health information about an individual
18 that is permitted by this title and not otherwise prohibited
19 by State or Federal statute shall not be liable to the indi-
20 vidual for the disclosure under common law.

21 (g) NO LIABILITY FOR INSTITUTIONAL REVIEW
22 BOARD DETERMINATIONS.—If the members of an institu-
23 tional review board have in good faith determined that a
24 health research project is of sufficient importance so as
25 to outweigh the intrusion into the privacy of an individual

1 pursuant to section 128(a)(1), the members, the board,
2 and the parent institution of the board shall not be liable
3 to the individual as a result of such determination.

4 (h) GOOD FAITH RELIANCE ON CERTIFICATION.—A
5 health information trustee who relies in good faith on a
6 certification by a government authority or other person
7 and discloses protected health information about an indi-
8 vidual in accordance with this title shall not be liable to
9 the individual for such disclosure.

10 **SEC. 162. CIVIL MONEY PENALTIES.**

11 (a) VIOLATION.—Any health information trustee who
12 the Secretary determines has substantially failed to com-
13 ply with the provisions of this Act shall be subject, in addi-
14 tion to any other penalties that may be prescribed by law,
15 to a civil money penalty of not more than \$10,000 for
16 each such violation.

17 (b) PROCEDURES FOR IMPOSITION OF PENALTIES.—
18 The provisions of section 1128A of the Social Security Act
19 (other than subsections (a) and (b) and the second sen-
20 tence of subsection (f)) shall apply to the imposition of
21 a civil monetary penalty under this section in the same
22 manner as such provisions apply with respect to the impo-
23 sition of a penalty under section 1128A of such Act.

1 **SEC. 163. ALTERNATIVE DISPUTE RESOLUTION.**

2 (a) IN GENERAL.—The Secretary shall, by regula-
3 tion, develop alternative dispute resolution methods for
4 use by individuals, health information trustees, and other
5 persons in resolving claims under section 161.

6 (b) METHODS.—The methods under subsection (a)
7 shall include at least the following:

8 (1) ARBITRATION.—The use of arbitration.

9 (2) MEDIATION.—The use of mediation.

10 (3) EARLY OFFERS OF SETTLEMENT.—The use
11 of a process under which parties make early offers
12 of settlement.

13 (c) STANDARDS FOR ESTABLISHING METHODS.—In
14 developing alternative dispute resolution methods under
15 subsection (a), the Secretary shall ensure that the meth-
16 ods promote the resolution of claims in a manner that—

17 (1) is affordable for the parties involved;

18 (2) provides for timely resolution of claims;

19 (3) provides for the consistent and fair resolu-
20 tion of claims; and

21 (4) provides for reasonably convenient access to
22 dispute resolution for individuals.

23 **SEC. 164. AMENDMENTS TO CRIMINAL LAW.**

24 (a) IN GENERAL.—Title 18, United States Code, is
25 amended by inserting after chapter 89 the following:

1 **“CHAPTER 90—PROTECTED HEALTH**
 2 **INFORMATION**

“Sec.

“1831. Definitions.

“1832. Obtaining protected health information under false pretenses.

“1833. Monetary gain from obtaining protected health information under false pretenses.

“1834. Knowing and unlawful obtaining of protected health information.

“1835. Monetary gain from knowing and unlawful obtaining of protected health information.

“1836. Knowing and unlawful use or disclosure of protected health information.

“1837. Monetary gain from knowing and unlawful sale, transfer, or use of protected health information.

3 **“§ 1831. Definitions**

4 “As used in this chapter—

5 “(1) the term ‘health information trustee’ has
 6 the meaning given such term in section 3(b)(3) of
 7 the Fair Health Information Practices Act of 1994;
 8 and

9 “(2) the term ‘protected health information has
 10 the meaning given such term in section 3(a)(3) of
 11 such Act.

12 **“§ 1832. Obtaining protected health information**
 13 **under false pretenses**

14 “Whoever under false pretenses—

15 “(1) requests or obtains protected health infor-
 16 mation from a health information trustee; or

17 “(2) obtains from an individual an authoriza-
 18 tion for the disclosure of protected health informa-
 19 tion about the individual maintained by a health in-
 20 formation trustee;

1 shall be fined under this title or imprisoned not more than
2 5 years, or both.

3 **“§ 1833. Monetary gain from obtaining protected**
4 **health information under false pretenses**

5 “Whoever under false pretenses—

6 “(1) requests or obtains protected health infor-
7 mation from a health information trustee with the
8 intent to sell, transfer, or use such information for
9 profit or monetary gain; or

10 “(2) obtains from an individual an authoriza-
11 tion for the disclosure of protected health informa-
12 tion about the individual maintained by a health in-
13 formation trustee with the intent to sell, transfer, or
14 use such authorization for profit or monetary gain;
15 and knowingly sells, transfers, or uses such information
16 or authorization for profit or monetary gain shall be fined
17 under this title or imprisoned not more than 10 years, or
18 both.

19 **“§ 1834. Knowing and unlawful obtaining of pro-**
20 **tected health information**

21 “Whoever knowingly obtains protected health infor-
22 mation from a health information trustee in violation of
23 the Fair Health Information Practices Act of 1994, know-
24 ing that such obtaining is unlawful, shall be fined under
25 this title or imprisoned not more than 5 years, or both.

1 **“§ 1835. Monetary gain from knowing and unlawful**
2 **obtaining of protected health information**

3 “Whoever knowingly—

4 “(1) obtains protected health information from
5 a health information trustee in violation of the Fair
6 Health Information Practices Act of 1994, knowing
7 that such obtaining is unlawful and with the intent
8 to sell, transfer, or use such information for profit
9 or monetary gain; and

10 “(2) knowingly sells, transfers, or uses such in-
11 formation for profit or monetary gain;

12 shall be fined under this title or imprisoned not more than
13 10 years, or both.

14 **“§ 1836. Knowing and unlawful use or disclosure of**
15 **protected health information**

16 “Whoever knowingly uses or discloses protected
17 health information in violation of the Fair Health Infor-
18 mation Practices Act of 1994, knowing that such use or
19 disclosure is unlawful, shall be fined under this title or
20 imprisoned not more than 5 years, or both.

21 **“§ 1837. Monetary gain from knowing and unlawful**
22 **sale, transfer, or use of protected health**
23 **information**

24 “Whoever knowingly sells, transfers, or uses pro-
25 tected health information in violation of the Fair Health
26 Information Practices Act of 1994, knowing that such

1 sale, transfer, or use is unlawful, shall be fined under this
2 title or imprisoned not more than 10 years, or both.”.

3 (b) CLERICAL AMENDMENT.—The table of chapters
4 for part I of title 18, United States Code, is amended by
5 inserting after the item relating to chapter 89 the
6 following:

“90. Protected health information 1831”.

7 **TITLE II—AMENDMENTS TO**
8 **TITLE 5, UNITED STATES CODE**

9 **SEC. 201. AMENDMENTS TO TITLE 5, UNITED STATES CODE.**

10 (a) NEW SUBSECTION.—Section 552a of title 5,
11 United States Code, is amended by adding at the end the
12 following:

13 “(w) MEDICAL EXEMPTIONS.—The head of an agen-
14 cy that is a health information trustee (as defined in sec-
15 tion 3(b)(3) of the Fair Health Information Practices Act
16 of 1994) shall promulgate rules, in accordance with the
17 requirements (including general notice) of subsections
18 (b)(1), (b)(2), (b)(3), (c), and (e) of section 553 of this
19 title, to exempt a system of records within the agency, to
20 the extent that the system of records contains protected
21 health information (as defined in section 3(a)(3) of such
22 Act), from all provisions of this section except subsections
23 (e)(1), (e)(2), subparagraphs (A) through (C) and (E)
24 through (I) of subsection (e)(4), and subsections (e)(5),

1 (e)(6), (e)(9), (e)(12), (l), (m), (n), (o), (p), (q), (r),
2 and (u).”.

3 (b) REPEAL.—Section 552a(f)(3) of title 5, United
4 States Code, is amended by striking “pertaining to him,”
5 and all that follows through the semicolon and inserting
6 “pertaining to the individual;”.

7 **TITLE III—REGULATIONS; EF-**
8 **FECTIVE DATES; APPLICABIL-**
9 **ITY; AND RELATIONSHIP TO**
10 **OTHER LAWS**

11 **SEC. 301. REGULATIONS.**

12 Not later than July 1, 1996, the Secretary shall pre-
13 scribe regulations to carry out this Act.

14 **SEC. 302. EFFECTIVE DATES.**

15 (a) IN GENERAL.—Except as provided in subsection
16 (b), this Act, and the amendments made by this Act, shall
17 take effect on January 1, 1997.

18 (b) PROVISIONS EFFECTIVE IMMEDIATELY.—Any
19 provision of this Act that imposes a duty on the Secretary
20 shall take effect on the date of the enactment of this Act.

21 **SEC. 303. APPLICABILITY.**

22 (a) PROTECTED HEALTH INFORMATION.—Except as
23 provided in subsections (b) and (c), the provisions of this
24 Act shall apply to any protected health information that
25 exists in a State on or after January 1, 1997, regardless

1 of whether the information existed or was disclosed prior
2 to such date.

3 (b) SPECIAL PURPOSE TRUSTEES.—The provisions
4 of this Act shall not apply to any special purpose trustee,
5 except with respect to protected health information that
6 is received by such a trustee on or after January 1, 1997.

7 (c) AUTHORIZATIONS FOR DISCLOSURES.—An au-
8 thorization for the disclosure of protected health informa-
9 tion about an individual that is executed by the individual
10 before January 1, 1997, and is recognized and valid under
11 State law on December 31, 1996, shall remain valid and
12 shall not be subject to the requirements of section 122
13 until July 1, 1998, or the occurrence of the date or event
14 (if any) specified in the authorization upon which the au-
15 thorization expires, whichever occurs earlier.

16 **SEC. 304. RELATIONSHIP TO OTHER LAWS.**

17 (a) STATE LAW.—Except as provided in subsections
18 (b) and (c), this Act shall prevent the establishment, con-
19 tinuing in effect, or enforcement of State law to the extent
20 such law is inconsistent with a provision of this Act, but
21 nothing in this Act shall be construed to indicate an intent
22 on the part of Congress to occupy the field in which its
23 provisions operate to the exclusion of the laws of any State
24 on the same subject matter.

1 (b) PRIVILEGES.—This Act does not preempt or mod-
2 ify State common or statutory law to the extent such law
3 concerns a privilege of a witness or person in a court of
4 the State. This Act does not supersede or modify Federal
5 common or statutory law to the extent such law concerns
6 a privilege of a witness or person in a court of the United
7 States.

8 (c) CERTAIN DUTIES UNDER STATE OR FEDERAL
9 LAW.—This Act shall not be construed to preempt, super-
10 sede, or modify the operation of—

11 (1) any law that provides for the reporting of
12 vital statistics such as birth or death information;

13 (2) any law requiring the reporting of abuse or
14 neglect information about any individual; or

15 (3) subpart II of part E of title XXVI of the
16 Public Health Service Act (relating to notifications
17 of emergency response employees of possible expo-
18 sure to infectious diseases).

○

Mr. CONDIT. We have with us this morning a member who has agreed, and I'm delighted to have her as a coauthor, a significant coauthor and a strong supporter of this concept and this legislation, and she's here this morning. If Mr. Thomas wouldn't mind, I'm going to let her testify before we move to additional opening statements.

Ms. Velázquez represents the 12th District of New York and is a cosponsor. She will share with us this morning her own story about the improper disclosure of sensitive health information.

This morning we will also receive testimony from the Clinton administration, represented by Nan Hunter, deputy general counsel at the Department of Health and Human Services, and we will also hear from a public opinion poll on health privacy issues. Equifax has performed an important public service by sponsoring this very timely survey. Equifax is represented today by Mr. Baker, who is senior vice president, and we're delighted to have him here and welcome his participation in this issue.

The analysis will be provided by Professor Alan Westin of Columbia University. Professor Westin is one of the leading privacy scholars. He's conducted the first study on computer and health records in 1976.

And I'm going to have to kind of back up just a little bit before we allow my colleague to make her opening statement and welcome the chairman of the full committee here this morning and tell him that we welcome him and appreciate his interest in this issue and thank him for allowing us to proceed ahead in this area, and let him make any statement that he cares to make. Chairman Conyers.

Mr. CONYERS. Thank you very much, Chairman Condit. And my colleagues on the subcommittee, good morning.

We're delighted that Ms. Velázquez will be our first witness because this bill, and I'm very happy to be associated with it, is a landmark bill. For the first time, we're putting together some rights and responsibilities in keeping the most sensitive of information that is maintained by our citizens, namely, health care information.

The bill was put together with a group of people interested in this subject, and I am absolutely delighted that it has come out in the form that it has. And I want to commend the chairman because in the information age, these records are now becoming more easy to be misused, and we're providing the first protections.

And this is an important part of jurisdiction of the Government Operations on the health care bill. It will be coming forward as a single free-standing bill, so it isn't going to turn on which particular measure ultimately succeeds in the three committees.

I'm pleased that I can be here merely to identify how strongly I support it and will be looking forward to working with you, your subcommittee and the witnesses as we move this forward. Thank you very much.

[The prepared statement of Mr. Conyers follows:]

STATEMENT OF THE HONORABLE JOHN CONYERS, JR.
CHAIRMAN
COMMITTEE ON GOVERNMENT OPERATIONS

I would like to thank the Gentleman from California, Mr. Condit, for his hard work on this important legislation. H.R. 4077, of which I am proud to be an original cosponsor, is really a landmark bill. The bill comprehensively addresses the health care records of every American and offers both the promise of privacy and the assurance of accuracy. Medical records are among the most private and the most sensitive of any information maintained on our citizens. The deliberate or inadvertent release or misuse of these records can have catastrophic consequences for individuals. Congresswoman Valazquez will testify about that, if anyone has any doubts.

In addition to guaranteeing privacy for medical records, the bill accords certain rights to individuals to ensure that their medical records are accurate, timely, relevant, and complete. Individuals will be able to inspect their records and make corrections or additions.

As we move into the information age, and as records become more computerized and more easily misused, this bill will provide the protections required to ensure the privacy of medical records. Insurance, employment, and other important decisions made on the basis of medical records which a patient has not agreed to disclose is a real threat to every American. Similarly, if decisions are made on the basis of faulty information contained in medical records, the damage can be just as serious.

This bill is a valuable contribution to the health care debate in this country. No matter what type of system is finally agreed upon by this Congress, this legislation will be an essential component. It has been developed in close consultation with experts on medical issues and privacy, and I hope that it receives the strong support of the Administration that it deserves. I commend Mr. Condit for his efforts.

Mr. CONDIT. Thank you, Mr. Chairman.

Ms. Velázquez is, as I mentioned, a representative from the 12th District of New York and we're honored and delighted to have you here this morning. I really appreciate your support and participation. Thank you.

**STATEMENT OF HON. NYDIA VELÁZQUEZ, A REPRESENTATIVE
IN CONGRESS FROM THE STATE OF NEW YORK**

Ms. VELÁZQUEZ. Good morning, Mr. Chairman, and members of the committee. I would like to thank you, Mr. Chairman, for convening this very important hearing and for giving me the opportunity to testify.

Let me begin by stating that the only reason I have the strength to come here before you today and discuss this very difficult personal experience is because of the outpouring of love and support from my friends and constituents since its occurrence. I am indebted to them for standing behind me in my hour of need.

Mr. Chairman, technology is a double-edged sword. It provides us with more efficient ways to store and disseminate information, but it also poses significant problems in controlling access to sensitive data.

As policymakers, we should support the development of new technologies, such as the information superhighway, which improve our quality of life, but we must protect the rights of individuals, especially in the area of privacy.

With the existence of such entities as the Medical Information Bureau, which was created by insurers to reduce fraud, and which contains information on 80 percent of health insurance policies in the country, and with State motor vehicle departments sending information, it is very hard to keep sensitive data from ending up in the wrong hands.

During my campaign for Congress, I realized that no one is immune to privacy violations. I had my private, personal medical records leaked to the newspapers in New York City. Every time I talk about this I relive it. The story of my experience is very difficult for me to discuss, knowing the stereotypes that exist regarding mental illness.

A few years ago I sought needed medical treatment after a suicide attempt. I went to the hospital confident that I will receive treatment and that my experience will be private, between me and my doctor.

Let me explain to you what happened to me 1 year later. I had just been through the most difficult challenge of my life. For 4 grueling months I walked the streets of my district, campaigning to represent the people of the 12th Congressional District in Congress.

I went up against an 18-year incumbent with a vast war chest. In addition, there were four other Latino candidates in the race. The conventional wisdom was that one Latino couldn't win against those odds.

Well, I beat the odds. For a Puerto Rican woman from a community that has little money and few resources, there were tremendous odds.

Just imagine what I felt 3 weeks after I won this victory in the primary when I woke up one morning with a phone call from my friend, Pete Hamill, a reporter at the New York Post. He told me that the night before, the Post has received an anonymous fax of my records from St. Claire Hospital. The records showed that I had been admitted to the hospital 1 year ago seeking medical assistance for a suicide attempt.

He told me that the other newspapers across the city had received the same information and the New York Post was going to run a front page story the next day. For the press, it was a big story. For me, it was a humiliating experience over which I had no control.

How ironic that 3 weeks before, when I won the primary, I did not make the front page of the New York Post, but my suicide attempt of 1 year ago did. My records were leaked for one purpose only: To destroy my candidacy for the U.S. House of Representatives by discrediting me in the eyes of my constituents.

Very few people knew about my situation, and I made the decision of not sharing it with my family. I wanted them to always remember me as a fighter—happy and strong. My father and mother, 80 years old, they did not understand, and they still do not understand.

When I found out that this information was being published in the newspaper and that I had no power to stop it, I felt violated. I trusted the system and it failed me. What is most distressing is that once medical records leave the doctor's office, there are no Federal protections to guard against the release of that information.

In some States it is easier to access a person's medical record than it is to obtain the records of a person's video rentals.

After my experience, many people approached me and told me of their fears that records of their doctors' visits could be made public if they sought treatment for mental illness. It is this fear of being discriminated against that prevents people from seeking the treatment that they need. This fear also speaks to the larger issue of the stigmas attached to mental illness and treatment for mental illness.

Part of the Hippocratic oath reads, "Whatsoever things I see or hear concerning the life of man, in any attendance on the sick or even apart therefrom, which ought not be voiced about, I will keep silent thereon."

I realize that laws governing disclosure of medical records vary from State to State, but it is distressing that sometimes all medical professionals do not abide by that part of the oath.

I do not profess to be an expert on all the legal ramifications of comprehensive privacy legislation, but I do believe that we need stringent, uniform, and thorough standards for the disclosure of medical records, with the necessary medical and legal exceptions that must be adhered to by all medical practitioners and administrators.

I appeal to everyone not as a politician but as a victim, someone whose personal medical records were released to the press and the public without approval or even advanced notice, someone who has

experienced the pain and lingering effects of having intimate personal information exploited.

We must preserve an important historic principle underlying patient care: The preservation of confidentiality, the privacy and security of sensitive personal information.

President Clinton's Health Security Act, H.R. 3600, contains medical record and privacy provisions which are an important first step toward protecting the innocent victims from the unscrupulous use of medical records, but they need improvement.

In the area of privacy, the bill only provides for the development and implementation of a health information system which would enable a National Health Board to collect, report and regulate the dissemination of health information. The President's bill further authorizes the same board to set standards regarding the privacy of individually identifiable health information.

The problem is that the bill provides no clues or guidelines as to what the standards should be or how they plan to reconcile the future standards with the various State rules regarding disclosure of medical information.

Furthermore, the technological improvements to the collection and storage of medical information which the President proposes, such as the computerization of medical records and implementation of a health security card, drastically increases the number of individuals with access to private medical information.

I recognize that computerization may lead to reduced medical costs, facilitate exchange of information between medical professionals and prevent fraud, but computerization also increases the likelihood that an individual or group will attempt to obtain such information without the consent of the patient.

Despite the problems that I have outlined regarding the storage and disclosure of medical information, there is hope. That hope springs from the efforts of Chairman Condit and his introduction of H.R. 4077, the Fair Health Information Practices Act of 1994.

I am proud to say that I am an original cosponsor of this very important piece of legislation. H.R. 4077 will establish uniform, comprehensive Federal rules governing the use and disclosure of identifiable health information and specify the responsibilities of those who collect, use, and maintain health information. The bill also will provide criminal penalties for privacy violations and give patients the right to sue for damages. It is my sincere hope that the Congress supports this measure.

Mr. Chairman, I am one of the lucky ones, for a number of reasons. First, I was able to afford the treatment that I needed to recover. It frightens me to think how many people suffer in depression and despair because they cannot afford the professional services or medicine that can make them whole again.

Second, I received a great deal of support from my community, and luckily did not have my credibility diminished in their eyes. Most people are not so lucky. Most people are forced, because of the fear and social stigma attached to mental illness, to not seek medical treatment. Further, the release of their medical records, if they seek treatment, could cripple their chances for credit or work or social acceptance.

It is important for you to recognize, Members of Congress, that the only reason I am able to testify about this experience, as a productive member of society, is because I had the strength of will, the financial means and the support of my community.

And speaking of support, I want to take this opportunity to express my appreciation and gratitude to Tipper Gore, the Vice President's wife, for all of her commitment, compassion, and work on behalf of mental illness. I personally shared my experience with her and she has been very sensitive and supportive.

Mr. Chairman, I would like to commend you for your dedication and hard work on the issue of privacy. I sincerely hope that our colleagues will join us not only in working diligently to pass H.R. 4077 but also in addressing the larger issue of mental illness. Thank you.

Mr. CONDIT. Thank you very much. I would like to commend you for being here and sharing your personal story. You're very courageous to do that, and it's extremely helpful for this committee and for the Congress to understand the issue.

I believe most Americans would be surprised and not especially pleased if they knew that they may be in the same kind of circumstances, that their information is available and could be used, and used in a way that wouldn't be helpful to them. So it's very helpful for you to be here.

One of the premises of the bill is that both doctors and patients are confused about confidentiality rules. Do you agree that a uniform set of rules would help to lessen the confusion and bring about better compliance?

Ms. VELÁZQUEZ. Yes, sir. I totally agree, Mr. Chairman. As I pointed out in my testimony, uniform Federal guidelines for the protection of a person's medical record, it is a must if we want to guarantee that the rights of people will be protected, and also that patients will not fear when they are in need, for seeking professional help.

Mr. CONDIT. What has been the public reaction to the disclosure of your private health records? Did it make people nervous that their own records are vulnerable to improper disclosure?

Ms. VELÁZQUEZ. Definitely. Many people approached me in the streets and some of them shared with me that they have gone through the same kind of experience that I have gone through, and they expressed their fear, that they don't feel that there is any protection for them to feel comfortable enough in seeking professional help.

Mr. CONDIT. So actually, it's kind of a double problem because people live in fear that someone would disclose it, and it also would keep them from going in and getting help to help themselves, right?

Ms. VELÁZQUEZ. Well, even myself now. Whenever I need, I have to go and see a doctor, it's just that it comes back to me. It's haunting me.

Mr. CONDIT. H.R. 4077 proposes stiff criminal penalties for violations. It also provides for civil lawsuits against those who improperly disclose protected health information. Will these stiffer remedies serve as a deterrent in the misuse of health information, in your opinion?

Ms. VELÁZQUEZ. I cannot say here that it will solve all the problems regarding privacy, but at least people will feel more comfortable. And also, those who might think of revealing this type of information will think twice before they do it.

Mr. CONDIT. Mr. Thomas, do you have any questions? Or do you want to make your opening statement now? You're welcome to do so.

Mr. THOMAS. Well, let me just have one question. I appreciate very much your being here and your testimony.

As you reviewed this circumstance, do you think this was a breach of a system that's now in place or the lack of regulations? Wasn't it wrong for this to be released under the current ethics, at least, and rules?

Ms. VELÁZQUEZ. It was wrong but I think that we need to have uniform guidelines at the Federal level because, as we know right now, it is the States—it will vary from State to State.

Mr. THOMAS. Your experience was within your own community.

Ms. VELÁZQUEZ. I don't understand.

Mr. THOMAS. Interstate has little to do with your particular experience.

Ms. VELÁZQUEZ. I know, but I think that the lack of protection that exists and the fact that we don't have any Federal laws governing this, you know, people think that they could get away with this.

Mr. THOMAS. OK, thank you.

Mr. CONDIT. Mr. Horn.

Mr. HORN. Could I yield to my colleague?

Mr. CONDIT. Absolutely.

Ms. ROS-LEHTINEN. Thank you. Thank you, Congressman Horn, and thank you, Mr. Chairman.

It's a pleasure for me to be here today and listen to the very moving and courageous and dignified, professional yet very heartfelt testimony of my dear friend, Nydia Velázquez, who is certainly a role model, not only for the young women in her district, but I can tell you that she's a role model for the young women in my district who know who Nydia Velázquez is and look up to her, as she is a role model for all Hispanic young ladies, especially.

And I'm very proud to say that she's my friend. It's been a pleasure for me working with her this short time that we've known each other. But certainly, Nydia, your words and your personal experience will change lives and will give hope to so many people who suffer with mental illness. And I'm very sure that your personal experiences will help others seek professional help, and it will not act as a deterrent.

The unfortunate campaign against you, I think, really as difficult as it was for you personally, will change lives forever. And I hope that it will not cause people to be deterred in seeking professional help but will actually help them in making that uncomfortable yet very important decision.

And I congratulate your constituents also in handling these disclosures correctly, putting them in the proper light, that they were just a political smear against you, and I know that you have made Congress a better place by you being here. And I hope that you will

continue to be with us for many years. I thank you for your testimony today.

Ms. VELÁZQUEZ. Thank you, Ileana, for those words.

Mr. CONDIT. Mr. Horn.

Mr. HORN. Thank you, Mr. Chairman. I join with what my colleague has just said.

I'm curious. Did they ever find out who released your records? Is that known?

Ms. VELÁZQUEZ. It's still under investigation by the DA in Manhattan so I cannot at this moment disclose any information regarding that matter.

Mr. HORN. So there are various laws of the State of New York that also apply?

Ms. VELÁZQUEZ. Oh, yes.

Mr. HORN. One of my concerns, and I wonder what your advice would be on it, is when you look at how medical records are kept, both in hospitals and in an office, what we're talking about is rather large organizations with a lot of employees have access. Each doctor seems to become a small business, given all the forms that one must fill out.

And as I've walked through both doctors' offices and hospitals, you often see a whole wall filled with files in some sort of order, either alphabetic or by case number. And the thought comes to mind as to how one pins responsibility on the protection of those records because almost any member of a changing staff might have access and pull out the record. You'd never even know it's gone because there are hundreds of other files on the same shelf, everything cramped together.

What's your thinking on that as to how responsibility might be pinned to protect records when so many people, who are fired or retired or leave with a grievance against their employer, have access to those records?

Ms. VELÁZQUEZ. Well, I am not an expert in terms of management, hospital management, but I think that it's the hospital's responsibility to make sure that a system is in place to protect the rights of people to privacy. And I understand what you're saying. There are many people who might have access, but they have to hold those people who have access responsible for their acts.

And ultimately, it's the hospital's responsibility.

Mr. HORN. Well, the real problem is when the act occurs, does anyone even know it's occurred until it hits the papers and you start tracing things back? So that's the thing you have to grapple with.

If I'm an employee and I have not been given a raise, I might be mad at the administrative section head in a hospital, the doctor in whose office I'm working, take some key files with me and use them for mischief and damage, just to hurt my employer. And so how do we deal with that problem?

Ms. VELÁZQUEZ. How do I deal with the pain of having my records released?

Mr. HORN. I take it there's no answer how we deal with that problem. Thank you, Mr. Chairman.

Mr. CONDIT. Ms. Woolsey.

Ms. WOOLSEY. I'm sorry that I missed my colleague's testimony, I just want you to know, as your colleague and your friend, I'm sorry that happened to you.

I'd like to respond to Mr. Horn. The hospital is the ultimate accountable entity at that point. If the hospital has a system that an employee, whether or not that employee is being mischievous or not, can get into patient files, it is that hospital's responsibility. This is what we have to be looking at.

Nydia, I just think you've been so brave, and thank you for sharing your experience with us so that we can learn from it and do everything we can to make sure it doesn't happen again, to anybody.

Ms. VELÁZQUEZ. Thank you.

Mr. CONDIT. Nydia, thank you very much. You're welcome to stay with us. I know you have a busy schedule, but we appreciate your support and help with this.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Mr. CONDIT. Let's do this, if we can. We have a journal vote and it started exactly 1 minute ago. Let me ask if any members have opening statements they'd like to make. Mr. Thomas.

Mr. THOMAS. Yes, sir, very briefly. First, let me thank you for calling today's hearing. I think as individuals and families become more mobile, protecting the privacy obviously is going to be a priority for this Congress, as we make changes in the health care program.

Protection of medical records is not simply a result of health care reform, however. With the development of advanced technology and the move toward computerization, records become more sensitive and the information bank, of course, has expanded.

Now that the President has proposed a massive government involvement in the health care system, confidentiality laws will become even more vital. On page 861 of the Health Security Act it requires doctors to report every patient visit to a national data base, along with their complete medical history.

It's difficult enough securing information as it flows through the various private payment and treatment processes, but it will be even more difficult once the Federal Government is in charge and people are carrying health security cards, perhaps with a chip in them, with their Social Security numbers on them.

The people of Wyoming do not want their lives open, as do the rest of the people, to a computer chip. That's why I look forward to these hearings and our witnesses regarding their assessment of 4077. I'd like to know how it coincides with the other current health reform proposals, because the administration's plan, of course, is not the only kid on the block, and indeed will probably not emerge as it came in.

Regional health alliances and national health boards are too complex, in my view, for people to swallow. So if the Congress changes these provisions, then how do we deal with this issue? And I think that's an important one.

So Mr. Chairman, I appreciate it and thank you for letting me participate in the hearings.

Mr. CONDIT. Mr. Horn.

Mr. HORN. I commend you, Mr. Chairman, for crafting this legislation and for holding 3 days of hearings, and I think in the course of that we'll try to look at all the ramifications of it.

Mr. CONDIT. Ms. Woolsey.

Ms. WOOLSEY. Thank you, Mr. Chairman. I'd like to thank you for introducing H.R. 4077 and addressing an issue of such great importance to every individual in this country—that's the privacy of personal health information.

And like my colleague, Representative Velázquez, has said, a person's medical records may contain the most private and intimate details of their life, details that only doctors and patients need to know.

So as technology advances we need to use that technology in order to protect confidentiality. We have a chance right now to do it right. So let's do it, and I look forward to working with you on H.R. 4077.

[The prepared statement of Ms. Woolsey follows:]

OPENING STATEMENT
INFORMATION, JUSTICE, TRANSPORTATION AND AGRICULTURE SUBCOMMITTEE
H.R. 4077
FAIR HEALTH INFORMATION PRACTICES ACT

CHAIRMAN CONDIT, I WOULD LIKE TO THANK YOU FOR INTRODUCING THE FAIR HEALTH INFORMATION PRACTICES ACT, H.R. 4077, AND FOR HOLDING TODAY'S HEARING.

H.R. 4077 ADDRESSES AN ISSUE OF GREAT IMPORTANCE TO EVERY INDIVIDUAL IN THIS COUNTRY--THE PRIVACY OF PERSONAL HEALTH INFORMATION.

A PERSON'S MEDICAL RECORDS MAY CONTAIN THE MOST PRIVATE AND INTIMATE DETAILS OF THEIR LIFE--DETAILS THAT ONLY DOCTOR AND PATIENT NEED TO KNOW.

AS TECHNOLOGY CONTINUES TO ADVANCE AT A RAPID PACE, WE WILL SEE NUMEROUS GREAT BENEFITS TO OUR HEALTH CARE SYSTEM. HOWEVER, ADVANCED TECHNOLOGY ALSO CREATES A SITUATION IN WHICH IT IS DIFFICULT TO REGULATE ACCESS TO PRIVATE HEALTH INFORMATION. I BELIEVE THAT WE MUST ADDRESS THE PROBLEMS ASSOCIATED WITH TECHNOLOGY AND AN INDIVIDUAL'S RIGHT TO PRIVACY WHILE CONTINUING TO SUPPORT EFFORTS TO CREATE INNOVATIVE TECHNOLOGIES.

CONGRESS MUST ENSURE THAT FAIR INFORMATION PRACTICES MUST BE INCLUDED IN THE HEALTH REFORM LEGISLATION THAT IS PASSED. WE WILL COMMIT A GREAT DISSERVICE TO THE AMERICAN PEOPLE IF WE DO NOT PROVIDE INDIVIDUALS WITH SUFFICIENT SAFEGUARDS REGARDING THE DISCLOSURE OF HEALTH INFORMATION. THAT'S WHY I BELIEVE THESE HEARINGS ON CHAIRMAN CONDIT'S BILL SO SIGNIFICANT.

I WOULD LIKE TO THANK OUR WITNESSES FOR BEING HERE TODAY. I LOOK FORWARD TO HEARING THEIR VALUABLE TESTIMONY.

THANK YOU, MR. CHAIRMAN.

QUESTIONS

Mr. CONDIT. Thank you very much. We're going to recess for a few minutes. We'll be back at approximately 10:20 to reconvene and Ms. Hunter will be our next witness.

[Recess taken.]

Mr. CONDIT. We'll reconvene. It is the policy of the subcommittee to swear in all our witnesses.

[Witness sworn.]

Mr. CONDIT. Thank you for your patience. The floor is yours.

**STATEMENT OF NAN D. HUNTER, DEPUTY GENERAL COUNSEL,
DEPARTMENT OF HEALTH AND HUMAN SERVICES**

Ms. HUNTER. Thank you very much, Mr. Condit. It's a pleasure to be here.

I want to begin by acknowledging the difficulty of following such dramatic and heartfelt testimony as that which was presented by Congresswoman Velázquez. But one thing I think that we can all agree on is the importance of the subject matter that we're discussing this morning.

We believe, as a number of persons have stated, that privacy protections at the Federal level are long overdue. The privacy law that exists now is skimpy, and there is no single, comprehensive, nationally applicable set of legal controls on health care information.

From the point of view of the administration, privacy protections are an integral part of the system, not just a luxury but a necessity. Privacy is a first principle of the administration's approach to health care reform.

We believe that if properly configured, privacy law can form the backbone for a health information system of the kind that we think is essential to health reform.

A health system that is as large and diverse and comprehensive as the American health care system needs the kind of careful and well designed controls that we are trying to formulate in the context of this legislation.

At the same time, these controls have to allow for the multiple important uses of information that the American people need. Reliable data are essential for research, for monitoring access, for public health, including the assessment of access by vulnerable populations, and for policing fraud and abuse in the system. And, of course, even the basic functions of payment and funds transfer cannot operate without an adequate information system.

As you know, the President's proposal for health care reform recognizes that confidentiality protections are essential for the system and for the information that flows through the system. It envisions the National Health Board issuing confidentiality guidelines within 2 years for the new information system, and within 1 year later proposing legislation that would be comprehensive.

Your bill offers immediate Federal legal protections for all health care records. We welcome this proposal and we're eager to work with you on it.

The committee and the staff have done an excellent job in formulating proposals for an area of law that is both extremely complicated and extremely important. We believe this is a real service to the Congress as we embark on health care reform, and we are extremely appreciative of that work.

The proposed legislation that you have introduced has requirements to carry out many of the same policy goals that are in the President's bill. Let me note where the two bills are consistent, because they're consistent on all the main, important principles.

They reassure patients that there are orderly processes for dealing with health care information. The duties provisions of your bill are especially important in that regard.

Your bill would require, as ours would, that individuals would have to be told of the intended uses of information about them. Under your bill there would be accounting of disclosures except in certain specified situations where that would not be appropriate, such as, for example, an ongoing law enforcement investigation.

Individuals would be able to see and get a copy of their records and offer corrections under both our bills.

There would be a basic protective requirement that any disclosures, even if authorized, would be limited to the minimum amount of information necessary to achieve their purpose. That would also be true under your bill for any authorized uses of information.

And all holders of records would have to establish strong security safeguards so that only authorized persons could have access to the records.

This is a situation, actually, where computers and computerization are quite helpful, in a situation like the one that Congresswoman Velázquez described. And in response to the question from Mr. Horn, we can prevent and track access to records that are held in computers in a much more efficient way than we can do now with paper records.

Both bills also call for remedies with teeth at the Federal level. These are fundamental principles regarding confidentiality of medical records, and we agree with you that they should be required by law.

Now, of course, one of our biggest concerns is how the proposed structure of your bill would interact with the larger information framework that we envision for health care reform.

One can think of health care information in two general categories. There is the universe of medical records, as we now know them, records that our doctors and hospitals keep on all of us, and some of those records can be quite extensive.

Second, would be, under health care reform, information in new systems that, apart from health care reform, are already being developed at State and community levels. That new information would not include or encompass the universe of medical records.

And here I want to correct a misimpression that was stated earlier. The President's bill does not call for the recording or the reporting of the universe of medical records to any central national data bank. Indeed, we don't envision any central national data bank of sensitive medical information.

We envision a network of data systems. The structure of our bill, in calling first for the board to promulgate regulations, would pertain to the new system geared to enrollment and claims data. And then we had envisioned legislation calling for regulation of the universe of records. You have gone ahead and proposed legislation regarding the universe of records. And, as I said, we welcome this and hope to work with you on it closely.

I want to describe the network of data systems briefly because it's relevant to our concerns regarding the bill that you have introduced.

We envision a system that includes uniform data standards that would be efficient and would produce enormous savings in the kind of duplicative recording and reporting for basic functions like claims and payment that exist now.

We do not require and the bill does not require or impose any requirement that all medical records be computerized. Obviously the system is moving in that direction, but that is not a requirement that's imposed by the President's bill.

What we envision is a data network in which certain core information that's necessary to operate the system would be transmitted, not a comprehensive national data base.

I want to address the health security card both because it's relevant to privacy and because it's important to correct misimpressions. It's a card that would be used from the consumer's point of view and the provider's point of view, to eliminate an enormous amount of paperwork and duplicative recording and reporting. At the point of service swiping the card would be the end of what is now an enormous amount of paperwork for the patient, and it would also enormously simplify what the individual physician or other provider had to do.

It is not set out in the President's bill as a smart card. It is not set out in the President's bill as being connected to any large data base. It would not increase access to sensitive medical information because the only information encoded on the card would be the information that was necessary to operate the basic function of accessing service and securing the payment and the record of that service.

The information in the new system, as I described that category before, would consist of enrollment data, obtained when people enroll in the system, and a minimum core data set of encounter data or claims data. The encounter data, as I said before, would not include all medical records, that universe of medical records that doctors have about all of us. And we do not envision all sensitive medical information being ever a part of the system or accessible by any kind of centralized computer access.

But this information system would have tremendously important and publicly beneficial functions. One is the research and statistical function by which the information system can produce aggregate information on the operation of the health care system, on who has access, on how it is utilized.

This kind of activity depends on access to the encounter data and enrollment data that would flow through the system, but does not use patient identifiers in its results and does not and should not be used to affect patients individually.

The body of information available from this data would be enormously valuable for research and statistical analysis about medical treatments, disease, access, and so forth. The compilation of the limited data that I've described could occur at regional data centers, which are described in our bill.

The configuration, the number and location of regional data centers will be determined when the system is implemented. That re-

gional data centers could be single, discrete entities. It's also possible that they could be a consortium of interests, either running a single data system or a network of data systems. This is already beginning at the State and local level.

But whatever their configuration, they would be capable of performing the research and statistical function and they would and should be subject to the same privacy standards as other entities.

We believe that the highest degree of protection under the law should be applied to the encounter data flowing to the regional data centers, when those data are used for research and statistical purposes.

Legal safeguards comparable to those which govern the Census Bureau could be appropriate for the research and statistical functions of regional data centers. By that, I mean that those functions could be immunized from the scope of reporting laws and judicial process, just as the Census Bureau is.

Individual providers would still be subject to the disclosure rules set out, for example, in your bill, so that they would be allowed to make the disclosures permitted for health use trustees, such as those, for example, for disease reporting, when a doctor reports disease to a public health authority.

But we believe that there are several key features that the committee might consider with regard to this special research and statistical function under health care reform. The committee might consider creating a different trustee class for entities that serve this function, tailored to provide explicitly for the appropriate rules for disclosure of data in the context of these functions, and providing additional protections beyond what your bill envisions, such protections that would ensure that such data would never be used in an inappropriate way against an individual, and that disclosures in the context of research, for example, would take place only when there was a demonstration that there was no practical way to conduct the research or statistical activity without identifiers and that there was a reasonable possibility of accomplishing the intended inquiry. The law should also make sure that the recipient had adopted security measures, and was using institutional review board procedures, and require researchers and other recipients to operate under the same principles.

This is the major suggestion that we want the committee to consider. Let me just briefly mention a few other areas where we want to draw the committee's attention.

One is the role of oversight and policing fraud and abuse. Your bill, as written, provides for disclosure of records for purposes of oversight, and we believe that's good and that's important. Units from my Department of Health and Human Services, such as the inspector general's office, and other units of the government are very involved in policing fraud and abuse, including some units in the Department of Justice and other entities.

When there is an investigation of fraud or abuse in the context of the health care system, we believe that the bill has to provide for appropriately protected disclosures, limited to those uses, as they would be in the bill, but which would not prevent that very important function from taking place.

The Department of Justice—both the Department of Health and Human Services and the Department of Justice, I might add, will be providing more detailed comments on the bill, and these are among the areas that we hope to work with you in the future.

Two other areas. One is preemption, an extremely difficult, complicated legal issue. Here I think one needs to consider several factors. One is that the protections that are provided in this bill and in State laws are important with regard to the ways in which, in the public health field, States have been able to develop specific procedures and specific reporting protections and processes.

One also needs to consider, however, that there is enormous benefit from a totally preemptive Federal standard for situations involving filing of claims electronically and other activities involving transmission of information. Especially in the area of payment and other kinds of financial information, the question of preemption is tremendously important.

Lastly, I want to just touch briefly on an area that comes up for many entities, including the Department of Health and Human Services, which actually operates systems of health care records, and that is the question of when the protections envisioned would terminate.

The traditional rule is that privacy protections terminate upon a patient's death. There has been some discussion of whether there should be some privacy protection that extends past the point of death.

We believe that the traditional rule is one which provides us and other health care providers a bright line that is necessary to anyone who administers a system of records. It is possible that some alteration of what that bright line is, such as an extension of 1 or 2 years, might be appropriate in some instances to protect against certain kinds of abuses, but what we feel is most important on this topic is clarify, and that any extension that be considered not be an extension past a reasonable amount of time.

Again, I want to emphasize how pleased we are that the committee has undertaken this work, how important it is and how important we view it, and we look forward to working with you.

[The prepared statement of Ms. Hunter follows:]



DEPARTMENT OF HEALTH & HUMAN SERVICES

Washington DC 20201

STATEMENT OF
NAN D. HUNTER, DEPUTY GENERAL COUNSEL
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
BEFORE
SUBCOMMITTEE ON INFORMATION, JUSTICE, TRANSPORTATION,
AND AGRICULTURE
COMMITTEE ON GOVERNMENT OPERATIONS
U.S. HOUSE OF REPRESENTATIVES

April 20, 1994

I am Nan Hunter, Deputy General Counsel, U.S. Department of Health and Human Services. I am happy to be here to discuss the bill you have introduced, H.R. 4077, to provide a code of fair information practices for health information.

The topic is vitally important and we are pleased that you share our vision for careful, respectful treatment of health information. Personally-identifiable health information is used for many purposes to benefit individuals and for broader societal needs. The challenge in legislating rules for confidentiality is always how to strike the best balance between those purposes and the rights of individuals. Let me begin by discussing the principles which underlie our concern for protecting health information.

The Reasons for Confidentiality

The primary goal of confidentiality in health care is to permit patients to be totally frank about facts which bear on their health, and to subject themselves to examination and tests which reveal facts about them. Without confidentiality protection, sick people would be faced with having to choose between revealing information to obtain treatment, or retaining their privacy -- a cruel choice, and one that would in some cases lead to untreated disease, or falsified information.

In public health and research there are equally pressing reasons: we want the patient to be frank not only for his or her own sake, but also for the health of society more generally. Only if we keep the patient's confidences will he or she be candid about sensitive matters. This permits us to intervene to protect others and interrupt the spread of communicable disease, and to gather accurate information for research about disease.

Ethical Principles

The traditions and ethical principles of the medical and other health care professions have long called for confidential handling of information about patients. For physicians, the obligation is found in the Hippocratic Oath, dating from the fourth century B.C., and is continued in current ethical statements. Other professions have similar ethical principles and codes of conduct. At the same time, the development of the health care system has led to use of records by many organizations that do not care for patients, and are not subject to the traditional ethical and social norms of the healing professions.

Legal Protections

Legal protections for health-care information today are skimpy and uneven at best, as the subcommittee is aware. They exist primarily at the state level, and they vary greatly. A few

states have comprehensive health-care information confidentiality statutes, including two (Montana and Washington) which have enacted the Uniform Health-Care Information Act of the National Conference of Commissioners on Uniform State Laws. Many have statutes covering particular types of information (like HIV-infection and mental health information), and some have statutes covering insurance information, including health information about beneficiaries. In addition, there is some case law establishing confidentiality duties.

The well-known physician-patient privilege (which most states have in some form), where applicable, applies only when the physician is asked to testify in court or in similar proceedings. It has nothing to do with decisions physicians or health care facilities make about disclosing patient information in other situations.

The only Federal health record confidentiality law covering the nation generally is one protecting information about patients in Federally-assisted drug and alcohol abuse treatment programs. The Privacy Act covers Federal records, including health records, held by Federal agencies that provide health care, such as the Department of Veterans Affairs, the Indian Health Service in the Department of Health and Human Services, and the military services. For health records of the Department of Veterans Affairs, two confidentiality laws apply, including one which provides specific protections for drug and alcohol, HIV infection, and sickle cell anemia records.

All these laws permit certain uses of patient information without the consent of the patient.

The array of existing laws provides some protection, but, as you know, there is no single, nationally-applicable set of legal controls on health care information.

Privacy Standards for an Information-Intensive System

A health care system as diverse and comprehensive as the U.S. health care system needs careful and well-designed controls on the use of information, to minimize risks to the privacy of patients. At the same time, these controls must allow for the appropriate use of information in providing health care to the American people.

Health records are used for many purposes today -- in the delivery of care to individuals, to operate the health care system, and for other purposes that are compatible with and related to the delivery of health care. People who work in a health care facility, in treating patients or in related activities like billing, need access to patient records.

Patients routinely authorize disclosure to health insurers to obtain reimbursement. Records are used for research to gain new knowledge to prevent and treat illness, often with patient identifiers so they can be linked with other records, although without further use or publication of the identifiers. Quality reviews and audits to assure that payments and reimbursements are correct require access to records. In some instances, medical conditions are reported to public health agencies, to permit investigation, and, as necessary, intervention. Health records frequently can be critical evidence in investigations and prosecutions of unscrupulous health care providers who defraud insurance programs, or deny their patients quality care.

Strong privacy protections can, if properly configured, form a backbone for the health information system that is essential to health reform. Legal controls of the type the subcommittee is considering prevent disclosures that are not appropriate or necessary. They reassure patients that there are orderly processes for dealing with their information, even if there is not absolute secrecy. They regulate government access to and use of information about people. They ensure that patients can see their own records if they wish, and provide remedies for patients whose records have been improperly used or disclosed.

Careful protections are especially important with the widespread computerization of records. Computerization can provide great benefits both for the patients and for management of the health care system. The effect on the privacy interests of patients is mixed. Computerized records present certain new vulnerabilities, such as the possibility that an unauthorized user may get access to them through the communications system. If an unauthorized user does get access, large volumes of information can be transmitted quickly and easily, while it is comparatively difficult to transmit large volumes of information in paper records.

At the same time, computerization can enhance privacy protection in many ways. For example, computerization makes it easier to pick out and disclose only information actually needed, rather than a patient's whole record. Further, when records are computerized, a more careful watch may be kept on their disclosure, through recording and auditing mechanisms built in to computerized record systems.

The Health Security Act

The President's proposal for health care reform, the Health Security Act (H.R. 3600) recognizes that clear and strong confidentiality protections are essential for the information that the new health care system will have about people, as well as for all the information traditionally held by health care providers.

The proposal envisions that the National Health Board will issue confidentiality rules, following principles of fair information practice set out in the President's bill, to protect personal data in the information network that the Board will establish to operate the system. For other records -- full medical records held by providers, for example -- the Board would be required to recommend confidentiality legislation to the President and Congress within three years.

Your bill offers immediate Federal legal protections for all health care records. We welcome this proposal, and are eager to work closely with you on it.

We are pleased that it has requirements to carry out many of the same basic policy goals set forth in the President's bill. Both bills share the following principles:

- * Individuals would have to be told of the intended uses of their information.
- * They would be able to see and get a copy of their records, and offer corrections.
- * There is a basic protective requirement that disclosures are to be limited to the minimum necessary to accomplish their purpose.
- * All holders of records would have to establish strong security safeguards, so that only authorized persons could have access to records.

These are fundamental principles for the confidential treatment of records about people, and we share your commitment to them. They should be required by law, and should also be instilled as part of the basic outlook of everyone who handles health information.

The uses and disclosures of information allowed for, and carefully controlled, by the bill, address many of the situations in which records are now used.

The remainder of my testimony will address areas of convergence and divergence in the bills, in the hope of being helpful to the subcommittee in its consideration of H.R. 4077. First, I will describe the national framework for health information that we believe is critical to achieving the basic goals of reform. Then I will address several of the larger conceptual issues where the Administration has concerns regarding H.R. 4077.

The Information Framework in the Health Security Act

The President's plan offers a new vision for a health information system that will empower consumers and relieve providers of the burdens of increasing and duplicative reporting requirements. We believe that H.R. 4077 as written is supportive of this information system, in that it attempts to establish the necessary disclosures, and to ensure that information so disclosed is protected from inappropriate further disclosure.

The national framework for health information described in title V of the Health Security Act is actually very simple. These are its key features:

- * The use of a health security card, to simplify administration for consumers and providers.
- * Uniform data standards, for reporting selected data items related to enrollment, claims, and encounters with health care professionals.
- * An electronic data network, through which selected items reported by alliances and health plans are collected, compiled, and transmitted to regional data centers, which can be configured in a number of ways.
- * Eventually, a point-of-service health information system that collects reportable data items as a by-product of the delivery of health care.

This framework will provide all participants in the health care system with accurate, comparable, and timely health information. Improving the quality and efficiency of the health care system depends on ready access to information. At the same time that the health care system depends on access to information to perform multiple, vital functions, we are developing ways to reduce the paperwork burden and simplify the administrative workings of the system. We can use technologies already in place to collect information once, and use a core data set for multiple purposes.

Some uses of information in the system will be administrative and operational. For example, information will be used to pay providers, to resolve issues of coverage, and to advise patients of their portion of costs.

In addition, the information system can have a research and statistical function: it can produce certain aggregate information on the operation of the health care system and on the health of our Nation. This activity depends on individual, identified

patient information, but does not use patient identifiers in its results, and does not affect patients individually.

Let me provide a few examples. National, uniformly-reported enrollment and encounter data provide unprecedented opportunities for many types of research, including clinical, outcomes, epidemiological, health services, and policy research. Enrollment offers the opportunity to collect a limited number of data items characterizing each individual (such as important sociodemographic factors). Encounter or claim data will provide a small, select number of elements characterizing encounters with practitioners, facilities, pharmacies, and laboratories (potentially including such elements as diagnosis, reason for service, service provided, site of service, provider, results, complications and charges).

Under the information system we envision, these data will be reported in the same way for all individuals and all encounters throughout the nation. Because it can be collected in a standard fashion across the nation, and will be comparable, it will be especially useful, and produce much better answers than more limited data from individual facilities, or particular states. The body of information available from these reports will be very valuable for research and statistical analysis -- to shed light on the operation of the health care system, to learn more about what medical treatments contribute most to improving health, to learn about the nature and course of particular disease conditions, and to document patterns of use of health care, and access to health care by various groups in the population.

The compilation of certain data will occur at regional data centers. The number, location, and organizational configuration of the data centers will be determined when the system is implemented. It is quite possible that regional data centers will be configured in a number of ways. Centers could be single discrete entities. A center could also be a consortium of interests that either runs a single data system or a network of geographically dispersed data systems. This flexibility would make it easier to build upon the existing data systems in a given region. Regardless of the configuration, all data centers would provide a minimum set of services and would be subject to the same privacy standards. Regional data centers would be electronically linked to facilitate access to information.

Implications of HR 4077 for the Health Information System

Data centers as envisioned under reform, as well as data utilities being considered under several state reform efforts, could have the research and statistical functions described above.

In performing those functions, they would receive certain encounter data, e.g., a minimum or core data set for visits with a physicians, but not the entire patient record. We believe that the highest degree of protection under the law should be considered for this information. Thus, we believe that legal safeguards comparable to those which govern the Census Bureau could be appropriate for the research and statistical functions of regional data centers. Those functions could be immunized from the scope of reporting laws and judicial process, just as the Census Bureau is. Individual providers would still be subject to the disclosure rules set out in the bill, so that they would be allowed to make disclosures permitted for health use trustees, such as those for disease reporting.

When encounter data are used for research and statistical purposes, they should not be used for actions against an identified individual. Limitation on the use of research and statistical information in this way -- called the principle of functional separation -- was recommended by the Privacy Protection Study Commission, in its report, Personal Privacy in an Information Society, in 1977, and the point was reiterated recently by a committee of the Committee on National Statistics in a report, Private Lives and Public Policies (1993).

Much health research can be conducted without patient identifiers. Computerization permits ready segregation of identifiers from other information about individuals, and public use files can be produced to permit extensive analysis in the many situations where it is not necessary to use identifiers to match health records with other records. But for research where records must be matched with other records, such as death certificates, identifiable information may be needed. With appropriate safeguards, this can be done with proper respect for privacy.

The committee might consider creating a special trustee class for entities that serve this function. A new section could be tailored to provide explicitly for disclosure of data for research and statistical purposes, and could provide additional protections for those data. This special class of information, (i.e., individually-identifiable health information when linked with other personal information) should not be used for all the purposes that the bill generally, and properly, allows for health oversight and payment agencies. We suggest consideration of the following restrictions on the use and disclosure of such data:

- * Personally-identifiable patient health information, once linked with other personal information for research and statistical purposes, should never be used to take any action affecting the rights, benefits, or privileges of an individual patient.

- * Such disclosures should take place only when there is a demonstration that there is no practical way to conduct the research or statistical activity without identifiers, that there is a reasonable possibility of accomplishing the intended inquiry, and that the recipient has adopted security measures to protect the information from any unauthorized redisclosure.
- * Disclosures should be made only following approval by a board, similar to the institutional board required in H.R. 4077 to review research disclosures. The board should be broadly representative (including members skilled in data and privacy issues) and should apply national standards in deciding whether to approve particular disclosures.
- * Researchers receiving identifiable data should not be allowed to disclose it further for any purpose, under the same penalties applicable to any other improper disclosure.

Oversight of the Health Care System

The bill as written provides for disclosure of records for the purposes of oversight. A wide variety of audit, investigative, and program evaluation activities require direct review of identifiable health records. In the vast majority of instances, the investigations are of health care providers, but there are some investigations of fraudulent actions by recipients with respect to payments for health care, and of collusion between patients and providers. These tasks are performed by the Office of Inspector General of the Department of Health and Human Services, by the Federal Bureau of Investigation, by other Federal investigative agencies, such as the Defense Criminal Investigative Service, the Offices of Inspectors General (including the Inspectors General of the Department of Labor, the Department of Veterans Affairs, the Office of Personnel Management and the Department of Defense), and by State and local agencies, including specialized Medicaid fraud units in states.

Among the issues that need attention to assure effective efforts against fraud and abuse are these:

- * Some investigations of fraud and abuse in the health care treatment and payment system are done by units of general law enforcement agencies, such as the Department of Justice, the Federal Bureau of Investigation, other Federal agencies such as the Drug Enforcement Administration and the U.S. Postal Inspector, and State and local police agencies. Additionally, there are civil and administrative as well as criminal enforcement agencies. Nearly every health care fraud investigation involves health records that would be covered by the bill.

These agencies use identifiable records from health care providers in the same way as specialized health oversight agencies, and access by such agencies ought not to be made more cumbersome than is strictly necessary to preserve patient privacy interests. We note that the bill provides that if these agencies get access as health oversight agencies, they may not use patient-specific information except in actions or investigations relating to receipt of or payment for health care.

- * While the bill provides for disclosure in connection with criminal activity or to determine if a crime has been committed, it is important to recognize that many investigations seek to determine whether civil fraud is occurring.
- * It might be desirable to simplify access for investigations of illegal activities not directly related to "receipt of health care or payment for health care", but involving health care in some fashion. Investigations of fraud in liability claims, disability program applications, or workers compensation claims need patient records.
- * Patient access to their own records in the hands of health oversight agencies, and patient awareness that their records have been disclosed by providers to investigative agencies, can in some instances reveal to patients that an investigation is underway, and permit evasive action. Existing subject access rights to Federal records, in the Privacy Act, include exceptions to address these concerns.

In connection with use and disclosure of records for investigations, the Department of Justice is preparing detailed comments on the bill and will provide them to the Committee soon.

Preemption

We note that the bill prevents the establishment or continuation of State law that is inconsistent with the bill's provisions, but does not occupy this field of law to the exclusion of State law. We interpret this to mean that the confidentiality rules would be cumulative. If a disclosure is prohibited by either this bill or State law, it would not be allowed, i.e., if State law prohibits a certain disclosure, that disclosure could not be made even if allowed by the Federal law, and if the Federal law prohibits a certain disclosure, that disclosure could not be made even if allowed by State law.

We appreciate the intention to let the State laws that offer stronger protections than this bill remain in place, especially with respect to especially sensitive types of health information. At the same time, we note the benefits of a totally preemptive

Federal law in situations involving the filing of claims electronically, and other activities involving transmission through national, computerized systems. Individual State requirements for patient authorization for disclosure, or review and approval processes, for example, can vitiate the benefits of standardized, automatic claims transmission.

Some consideration might be given to preempting State law totally for disclosures for payment of claims and related oversight activities and the health care information system. Other disclosures could be subject to both Federal and State law.

Living Patients and Deceased Patients

We note that the bill is silent on coverage of deceased persons. Most privacy statutes, including the Federal Privacy Act, do not apply to deceased persons. Substantial practical and administrative problems are created by confidentiality rules when there is no effective possibility of obtaining authorization from the patient. Approaches that rely on consent from next-of-kin or executors are difficult because such persons may not exist or may not be able to be found. In addition, the presumed protection may be meaningless because next-of-kin or executors may in some cases be the very people from whom the patient would have wanted to conceal information. However, even in the absence of legal protection, there are some safeguards:

- * Apart from situations where disclosure is legally compelled, holders of records have discretion not to reveal records.
- * To the extent that a record contains information about another, living, person, that information would be covered by the bill.

Use of Information Within an Organization

The bill includes a requirement that a health information trustee may use protected information only for a purpose that is compatible with and related to the purpose for which the information was collected or received. Restrictions on use -- restrictions on what can be done with information within an organization -- are important controls to assure that patient information is not used for other than its intended purpose, or seen by personnel who do not need it for their duties. Such restrictions become especially significant when an organization is large and carries out widely varied functions, such as the Department of Health and Human Services.

At the same time, it is important to allow for the ordinary supervisory mechanisms, necessary for accountability, in which persons not involved in direct health care, and having other, wider responsibilities, may need in some instances to see patient

records. Internal audits are such a case. In addition, it might be desirable to clarify the extent to which personnel of a facility conducting an activity such as research, using the facility's own records, must observe the same requirements that would have to be met for a disclosure outside of the facility.

Conclusion

We hope this testimony will prove helpful to the subcommittee. In addition to the points we have made here, we have additional technical comments which we would be pleased to offer as you continue work on the bill. We stand ready to answer any questions, and to help the subcommittee as needed.

Mr. CONDIT. Ms. Hunter, thank you very much. We look forward to working with you, and we appreciate very much your constructive testimony and suggestions this morning. I have a series of questions I'd like to ask you, and you can, if you want to in some cases, submit answers in writing later.

H.R. 4077 is a code of fair information practices that we can pass, we believe, this year. It looks a lot like the outline of the President's bill. Is there any reason not to pass this fair information practice bill this year?

Ms. HUNTER. Well, as I said, we welcome your proposal. It's different from how we approached it in the President's bill, but it's not inconsistent with the President's bill.

We had envisioned developing more specific standards simultaneously with the development of the information system, and we thought that that process would be aided by what we learned in developing the information system.

But we agree with you completely that standards, both for the new system and for the universe of medical records are extremely important, and we called for legislation. You've now drafted legislation, and so we're very, very happy to be involved in the process of working with you on it.

Mr. CONDIT. The use of identifiable health information by health researchers is supported in H.R. 4077, but there seems to be less public support for the notion. That's what the polls, the Equifax poll seems to indicate.

Can you make the case for the importance of identifiable health information for research, statistics? Also, statisticians want to have access to records. Should they be treated the same as researchers?

Ms. HUNTER. We believe that medical research is tremendously important and vital to the health of all Americans. And in thinking about it in privacy terms, one has to remember a couple of factors.

First, the benefits are enormous, and we all share in those benefits. But second, under your proposal and under the ideas that I've suggested in my testimony, there would be stringent protections against any kind of abuses harming to the individual, flowing from the use of information for medical research purposes.

There would be clear and stringent standards for approval of research protocols and for how any kind of information could be used. We are considering in our own discussions some of the mechanisms that are now available that allow even less disclosure while still permitting the research to go forward because of the possibilities that exist in certain kinds of computerized systems, for example.

When one balances the enormous benefits and the important stringent protections being in place, and I think the medical and the privacy communities are largely united on this point, medical research is an appropriate use, when one can assume those protections.

Let me just say one other thing about the Equifax poll. That was a fascinating document and I enjoyed reading it. I think that the questions that sought to elicit opinion about research were not able to place the question in the context of legal protection, because there isn't the kind of comprehensive Federal legal protection that your bill would provide and that we would support. And I think

public opinion would be affected by the knowledge of that kind of legal protection being in existence.

Mr. CONDIT. I'd like to go back to something you alluded to or made a statement about, the application of fair information principles to dead people. To cut off protection for records at the moment of death seems to be a bit harsh. Did I understand you to say continuing of full protection probably is unnecessary, but we should reach some agreement of 1 year, 2 years, 3 years?

Ms. HUNTER. It's one of those areas where you want to—you don't want to burden the system and the administration of records with regulations and rules that people can't practically administer, but I think you're right. It's possible that there could be abuses that would occur in some situations with a sort of instantaneous disclosure the moment after death.

As I said, if we could work with you on what a reasonable sort of short deadline would be, I think that would be a practical way to approach the situation.

Mr. CONDIT. I'm very concerned about the cost of legislation that we consider here in Congress. Would you estimate the cost of implementing H.R. 4077? Would it cost significantly more than the current patchwork quilt system of privacy rules? Would uniform Federal rules reduce the cost of transferring health data, especially in a computerized environment?

Ms. HUNTER. It's my understanding that absolutely having the uniform Federal rules on transmission of financially related data would result in a tremendous cost savings. And just having uniform rules that apply to most situations would ultimately lead, I think, to much greater efficiency.

One of the benefits for Federal health care entities is that operating under the standard of the Privacy Act, we have the benefit of a uniform Federal set of rules. It doesn't apply to anyone other than the Federal Government, but it gives us that benefit.

And the other situation that I think is relevant here is the context of health care reform, where if we can reform the payment system overall, there would be tremendous savings in administrative simplification, of the kind that I alluded to. And that, combined with a uniform set of rules, would make the overall system much more efficient.

Mr. CONDIT. Well, we would like to work with you and anyone else who has specific suggestions that could be made in the bill to reduce the cost. Do you see any right now that you could identify?

Ms. HUNTER. I can't identify now any specific provisions in your bill but I'd certainly be happy to get back to you on that.

Mr. CONDIT. Has the administration taken a position on the use of the Social Security number as an identifier for health records? If we have a clear set of fair information practice rules, does this type of identifier matter?

Ms. HUNTER. We have not taken a position on whether the Social Security number or some other number would be the identifier number in an integrated system. That is a matter that's still under study and that we're still considering and that Members of Congress may also want to consider.

Obviously the key concern here is a privacy related concern. There are other concerns, as well.

I think you're correct in pointing out that once we have a structure, a national system of confidentiality protections, we have to place our decision about the identifier number in the context of what that new structure would be.

And so I think it's very important to consider the two together.

Mr. CONDIT. The bill gives doctors discretion to disclose some health information to the patient's next of kin. This reflects current practice where doctors exercise judgment about what to tell the patient's spouse, except where the patient has objected.

This section has been controversial. Can you give us an opinion about it? Do we need to have written authorization before a doctor can make a routine disclosure to a spouse or next of kin?

Ms. HUNTER. This is a difficult area because you don't want to have the unusual case drive the entire system, but yet you want to have the law be flexible enough to recognize that there can be harm, significant harm, in the unusual case.

You certainly don't want to have a doctor who comes out of the operating room have to fear that she's going to be sued in Federal court if she walks out and tells people in the waiting room what happened during surgery.

I think it's one of those difficult to resolve issues, and we have not taken any formal position on that. I have reviewed the draft provision in your bill and it incorporates some safeguards in that section.

My suggestion would be that in those situations, that if there's a modification here, it should be directed to those situations where we anticipate the problems will occur; that is, where there is sensitive medical information involved and where the patient could conceivably herself or himself have indicated an unwillingness to have that information disclosed.

But in a routine situation, I think you have to allow the physician to communicate with the family members.

Mr. CONDIT. The bill permits the routine disclosure of information for purposes of treatment and payment without express authorization of the patient. This has been proposed because existing consent practices are especially meaningful.

Do you have any views on this?

Ms. HUNTER. Yes. The situation now often is that sometimes one is asked to sign a consent form and the consent form can be a very general and very blanket form.

I think what's important here, from a privacy perspective, is that the uses of the information be regulated and the disclosures of the information be regulated. It's more important to provide people meaningful protection of the sharing of their information than to have them sign a form that is simply a blanket form.

And I note that the part of your bill that does include consent forms does require very strong protections in terms of specificity. So that's a direction that we think is a good direction.

Mr. CONDIT. It's clear that the preemption section in this bill needs some work. How far can and should we go to preempt State law?

Ms. HUNTER. Well, as I indicated in my testimony, I think this is a situation where again, one should try and perhaps look at a preemption provision that would be tailored to certain functions.

Where you have financial functions involved, there's a tremendous need to have a single Federal rule so that all of the actors in the system don't have to comply with a lot of different rules, especially when claims information or payment information, for example, is transmitted across State lines.

On the other hand, in a very different area, you have some very highly developed State public health reporting laws, and I think that might be an area where Congress could consider permitting those States to continue with the public health schemes that they have already developed.

So I would encourage the committee to look at that kind of separation of functions with regard to the preemption provision.

Mr. CONDIT. Do you know of any States who may have a higher standard of protecting the information than we're proposing?

Ms. HUNTER. Well, the approach of your bill, I think correctly so, is that it permits certain disclosures but does not require those disclosures, in the area of public health, for example. And different States have specific provisions that sometimes prohibit disclosures that your bill might permit, but also often require disclosures of the kind that your bill permits but does not require.

And at that level of specificity for public health reporting, our tradition is that that's done at the State level, and I think it would be somewhat disconcerting to completely deviate from that tradition.

Mr. CONDIT. The regional health data organizations that you described in your testimony have both operational and research functions. Isn't it harder to write strict rules about the use of information when these functions are combined?

Ms. HUNTER. We are still thinking through what the possibilities would be for which functions should be combined at the regional data centers. We have in our institutional history, within the Department of Health and Human Services, precedence for entities like the National Center for Health Statistics or the HCFA data bases that are able to operate within the context of doing multiple functions. We are also considering whether to set apart those functions in a more distinct way.

So that's a matter that we're taking under careful consideration.

Mr. CONDIT. Ms. Woolsey.

Ms. WOOLSEY. Thank you, Mr. Chairman. I'm really impressed, Ms. Hunter, with your level and depth of knowledge on all of this. You're really a good resource for us.

I'm going to stay just on one subject. I'm of the belief that if we're going to have a universal card, that it would be a lot more cost effective, if we had a smart card from the beginning rather than a universal card at first and then, 5 years down the line, a smart card.

Can't we make a smart card now, with an upfront investment—an investment both in privacy and confidentiality? Couldn't we use a smart card to send medical data to regional research centers without using individuals names?

If we did that now, wouldn't that save time and give us the current information we need?

Ms. HUNTER. Let me clarify what I said before because perhaps I didn't explain it well enough. We do anticipate that encounter

data, not through the use of the health security card, but encounter data would be collected by regional data centers, as well as enrollment data, for example, that would provide demographic information. Encounter data would be the minimum——

Ms. WOOLSEY. Well, how are they going to get that? They're going to get paperwork.

Ms. HUNTER. Not through the card. I just want to separate the two because I think——

Ms. WOOLSEY. I think it could all be together, as long as we are willing to make an investment, which we're always afraid of.

Ms. HUNTER. Well, let me just try and make clear what I think we are doing, because I think it speaks to the main concern that you've expressed, and that is we are providing for data, core data set of encounter and enrollment data to go to regional data centers where, as I said in my testimony, regional data centers, one of the functions that they could perform is this research and statistical function.

That would give us the capability to have access to the incredibly rich kind of information about access and utilization and so on and so forth in health that I think we all want to have.

Ms. WOOLSEY. But that has to be done on a separate track. I mean, the physician, the office has to fill out another form.

Ms. HUNTER. No, she does not have to fill out another form. As we envision it, the health plans would forward information that is necessary for the financial mechanisms to operate, and that same core data set would be usable for these research functions, for quality assessment functions, for example.

So there would be the compilation once, at the plan level, of the core data set, of basic information about the encounter. And that one-time recording and compilation of information could be drawn upon for many different purposes—for payment purposes, for analysis purposes, for research purposes, as well.

So the research function and the other functions that you're concerned about are definitely functions that we believe are important for the system to provide. Just mechanically, that doesn't involve the use of the individual's card. The use of the card—you raise other important questions about that.

Ms. WOOLSEY. I have two ways to go with that. One, say there's an increase in breast cancer in a particular region. How are we going to track that?

Ms. HUNTER. We will track that through the information system that I described. That's exactly the kind of——

Ms. WOOLSEY. On an ongoing basis?

Ms. HUNTER. On an ongoing basis, because the diagnosis of breast cancer will be in the system through that core data set. We will be able to track that and we'll be able to know if there's a community in a specific area, for example, that has shown a sudden increase in breast cancer, an unexplainable, unusual sudden increase. That is the kind of better health outcome that we'll be able to achieve with a modern information system.

Ms. WOOLSEY. OK. What if I'm an individual that is allergic to some particular drug and I'd like to have that on my card so if I'm in an accident, somebody could know that immediately. Is that possible?

Ms. HUNTER. That's the question, the separate set of questions about the health security card, and they're important questions.

The President's bill does not envision and does not establish a card that has health information on it. That is correct. The bill, as currently drafted, does not include health information being encoded in the card.

We are considering what options might be available for that because in that area, you do have to balance the concerns of people who don't want health information on their card.

And the second point I would draw is that the technology of encoding certain information—and one could conceivably do this, you could encode certain information like allergies or emergency information—is very different from saying that the card would be usable to plug into a larger computer network.

And that second thing also is not part of the President's plan. We feel like the card is important for administrative simplification purposes. We're considering options, including perhaps an individual option, for allowing additional information to go on the card, but this is something that we're working on now.

Ms. WOOLSEY. Well, I think that would be the way to go, have a card now that could be expanded upon instead of having to start all over. If we're not prepared to ensure the protection of the privacy at this point, then we should not put all medical information on the universal card. But in the event that we will be able to ensure privacy in the future, and when we're ready, when we phase into that, then this same card should be able to be expanded. I really don't want to go back and start over at another date.

Ms. HUNTER. Well, I can assure you that efficiency and simplification are very important principles for us and we'll be happy to work with you in terms of what our thinking is now on the health security card.

Ms. WOOLSEY. OK, thank you very much. Thank you, Mr. Chairman.

Mr. CONDIT. Ms. Hunter, thank you very much.

Ms. HUNTER. Thank you.

Mr. CONDIT. You've been very helpful and we will be in contact with you.

Ms. HUNTER. Thank you, sir.

Mr. CONDIT. We have the next panel, Dr. Alan Westin, who is professor of public law and government at Columbia University and John Baker, senior vice president of Equifax, Inc., Atlanta, GA. Both these gentlemen have been with us all morning. We appreciate your patience, as well.

If you'll remain standing, we have a practice of swearing all witnesses in.

[Witnesses sworn.]

Mr. CONDIT. Let the record indicate they said, "I do," and who would like to go first? Mr. Baker, would you like to go first?

**STATEMENT OF JOHN BAKER, SENIOR VICE PRESIDENT,
EQUIFAX, INC., ATLANTA, GA**

Mr. BAKER. Yes, sir. Thank you. Thank you very much, Mr. Chairman. It's a pleasure to appear at this hearing. And, as you requested, the main focus of our testimony will be a discussion of

public opinion about health information privacy issues from our 1993 survey.

If this sequence is satisfactory, I'd like to just give a brief background to that survey, and then Dr. Westin will provide the findings in his analysis, and then perhaps I could make a few concluding comments with reference to your bill.

Mr. CONDIT. Absolutely.

Mr. BAKER. About several issues that we think might be important, several of which have already been discussed this morning.

We've submitted written testimony. The survey booklet has been distributed to subcommittee members. Dr. Westin has submitted copies of his testimony. We've also provided copies of an op-ed piece, which I might as well mention right up front, by our chairman, Jack Rogers, printed last week in the Washington Times, entitled "It's Time for Serious Legislation to Protect Medical Privacy."

And so I wanted to go quickly on the record, if I might, and say that we applaud the introduction of your Fair Health Information Practices Act of 1994, addressing a subject of considerable importance to the public. We agree very much with the statement that we have read that regardless of how the health delivery and payment system is restructured, there is and will continue to be a need for a code of fair information practices.

We do think it's time for national rules of the road for health information privacy. Your bill is an excellent beginning, in our opinion, and, as Chairman Conyers said, a landmark bill.

Let me back up for just a minute to say what Equifax is and what we do. We're a consumer information company. We work to help speed decisionmaking and facilitate business transactions in the economy, transactions such as consumer credit, check cashing, insurance underwriting, and, more recently, as our data base management and decision support expertise has grown, into newer areas involving health care payment transactions, medical bill audits and health system analysis.

Because we're a company that handles sensitive consumer information, we realize that for our long-run success, we do depend on public confidence in the integrity of our practices and in the stewardship of our information and the stewardship practices that we demonstrate.

We decided several years ago to undertake several or a number of privacy and consumer service initiatives, and they're referred to in our testimony and they're outlined in a booklet which is available here, which I would ask be included in the record, entitled "Consumer Information and Privacy, the Equifax Perspective."

Mr. CONDIT. Without objection.

[The information referred to follows:]

Consumer Information and Privacy

The Equifax Perspective

EQUIFAX



Introduction from the Chairman

C. B. Rogers, Jr., Chairman, CEO

For almost 100 years, Equifax has provided information services that help consumers obtain credit, insurance, employment and other benefits, while helping businesses and employers evaluate the risks and opportunities in such financial and employment transactions.

Our business customers rely on us for timely, accurate, and relevant information for risk assessment. Individual consumers expect that the information we supply about them will be accurate and will be provided only for legitimate business purposes. The economy depends upon current and precise information to assure effective and competitive transactions.

Throughout nearly a century of operations, as the needs of the marketplace and society's sense of appropriate standards for risk assessment have changed, Equifax has adapted its policies and procedures to reflect those changes. As new laws and regulations have been adopted to assure fair information practices in the consumer reporting industry, Equifax has led in their development and adheres to them in both letter and spirit.

Today, however, in an age of rapidly changing consumer services fueled by advanced information technology, companies such as ours must do more than follow the law to maintain the public's respect and merit consumers' trust. Leaders in our industry must learn, on the one hand, what consumers see as a fair balance between supplying information to businesses to obtain the services and benefits consumers seek from such businesses, while concurrently, on the other hand, respecting the consumer's legitimate rights to privacy. Businesses must then create operating policies and practices that support such fair balances, well before these may be written into law.

In the 1980s, Equifax created and published a code of fair information practices to reflect our commitment to operate as responsible stewards of the consumer information we collect and maintain. We committed ourselves to update and improve that code as changes in the marketplace and in social values might require.

This Equifax document reflects just such an updating of the Equifax fair information code for the 1990s. It explains our current role in connecting consumers and business, states our beliefs and policies about fair information uses, and explains the procedures and practices we follow to carry out our policies.

Most importantly, our Code epitomizes the continuing commitment of Equifax's 12,000 employees to provide the highest quality information for consumer services while adhering to the highest standards of fair information practices.

Equifax believes that individuals should have the following rights:

The right to be considered for credit, insurance, employment and other benefits on their own merits, based on their record of actions and performances.

The right to be treated with respect and fairness whenever information about them is used.

The right to privacy consistent with the requests and demands they make of business.

The right to have their applications for benefits or opportunities evaluated on the basis of relevant and accurate information.

The right to know what information has been provided about them for consumer reporting purposes.

The right to know what consumer data is being maintained about them and to be able to review the information in a reasonable time, at a charge that is not excessive, in a format that is understandable, and with an ability to challenge and correct inaccurate information.

The right to expect that information about them that is collected or stored for consumer reporting purposes will not be used for unanticipated purposes without notice or consent appropriate to the circumstances.

The right to expect levels of accuracy consistent with sound practices of record keeping and information systems management.

The right to have information about them safeguarded through secure storage, confidential handling within the organization, and careful transmittal to authorized and legitimate users.

The Role of Equifax: Information Stewardship

What does Equifax do?

Equifax helps people and businesses complete financial transactions.

Each year millions of people use credit cards, write checks, open charge accounts, apply for jobs, and insure their lives, health, homes and property. All these transactions require timely and reliable personal information. Equifax gathers such information, processes it, and transmits it to the banks, retailers, insurers, and other organizations that use it as the basis for granting these benefits.

What information do we gather?

The information that Equifax gathers must be relevant to the intended transaction and helpful to the decision-making process. In determining what information to report, Equifax draws upon custom, changing social values, and the needs of the marketplace. Equifax gathers and reports information that consumers and businesses recognize as necessary for the conduct of business.

For example, for a lender to approve a loan transaction, we provide information on a consumer's credit accounts, including the dates opened, dates of last activity, terms agreed to, balances, current status of accounts, and payment history.

For property or automobile insurance transactions, we provide information on the claims filed, including type of claims, identification of the policyholders, types of policies and insurance companies, status of claims, and amounts paid, where applicable.

Equifax does not gather or store information that has no bearing on the benefits for which a consumer is being considered. Consumers have the right to review the information, to ask questions, and to challenge and correct inaccurate consumer report information.

What do we do with this information?

Some information is gathered and stored on databases for retrieval when a financial transaction takes place. Often, we store and maintain information that is historical in nature and used repeatedly over time, such as a credit history. The best method of determining credit worthiness, for

example, is to know how a person has managed financial obligations in the past. In other cases, we may gather information on a one-time basis without retention to help a business make one specific determination — such as whether to employ an applicant or underwrite an automobile insurance policy.

How does Equifax benefit consumers, business and the economy?

Each day American consumers buy thousands of homes, cars, and major appliances. Most of these transactions are made on credit. The availability and reliability of credit history information makes it possible for these transactions to occur rapidly and efficiently.

Insurance premiums are more reasonable in cost because underwriters can obtain the necessary information to evaluate a person's application on his or her own merit. For example, life and health insurance underwriters, with a direct authorization by the consumer, can obtain from the consumer's attending physician a statement providing relevant information about the applicant's current and historical medical condition. Such medical information is not databased by Equifax.

Underwriters can also request Life & Health Underwriting Reports, which provide information needed to validate statements made on the insurance application. For the property and casualty insurance markets, Equifax offers an automated claims exchange database on automobile and property claims to help insurance companies evaluate the costs and risks of insuring drivers and motor vehicles. Information services also help reduce the costs of exaggerated or fraudulent claims.

Employers who use Equifax Employment Reports are better able to evaluate prospective candidates for particular job positions. These reports help confirm statements made by applicants and help employers protect the safety of employees, customers, and the public. They also help protect employers against substantial legal liability for negligent hiring.

Who can order or obtain consumer information?

First of all, the consumer, the subject of a report, has the right to know the contents of a report provided about him or her. Whether for credit, insurance, or employment, information gathered or reported by Equifax is available to the individual consumer. If a consumer questions any information in the report, we will recheck the information and make any corrections if there is erroneous or out-of-date information. If we can no longer confirm any particular information, we will remove it from the report. If we do confirm it, we will include the consumer's written statement about the information in question.

What legal requirements and voluntary practices govern our business?

The federal Fair Credit Reporting Act (FCRA) and various state laws govern the conduct of our business. Users of our services must comply with this legislation, which specifies punishment and fines for improper and illegal accessing of consumer report information. Federal and state laws do provide a basic framework for our information practices, but, in many instances, Equifax goes beyond the legal requirements to set additional standards and procedures in the interest of consumer service and privacy. For example, though not required by law, our practice is to provide consumers who have not been denied credit, insurance, or employment with detailed disclosure of all information in our file in easy-to-understand formats and with a system of toll-free access. Our information consultants are trained to provide quick and courteous service, and, whenever a recheck of information is requested, we follow up the process with a new, complete report.

We are permitted to furnish consumer reports only to those businesses having a permissible purpose — credit evaluation, insurance underwriting, employment decisions, the granting of a license, or other business needs involving a transaction with the consumer. To ensure that consumer report information is kept strictly confidential and is used only for permissible purposes, we carefully screen applications from businesses who want to receive consumer reports. We visit each applicant's premises to confirm identity and purpose of use, and we require every user to certify that reports will be requested in compliance with the aforementioned legal requirements.

New Realities of Consumer Information Services

INFORMATION FOR CONSUMER TRANSACTIONS has evolved from personal relationships between merchants and consumers in a local setting to a current global situation where financial transactions are between strangers, often located in different parts of the country or the world. As technology speeds up processes, consumers now expect loans and check approvals in minutes or seconds, rather than the several days or weeks that once were required.

In the past, consumer information services have provided information about consumers for business. Often consumers have not been active participants in the information process. Today, that is changing. Through several years of research and dialogue, we have recognized the growing importance of information to the individual and the importance of treating individuals as valued stakeholders in the consumer reporting process.

Information about consumers is also for consumers. Equifax wants to give people easy access to information reported about them and to foster understanding of the three-way consumer reporting process among the consumer, benefit granter, and Equifax, the reporting agency. Our goal is to deliver high quality, personal service to individuals on whom we maintain information and to provide that service in a manner that goes well beyond the letter of the laws which guide the information industry.

The New Emphasis on Individual Rights

OUR CONSUMER SERVICE GOALS have been based in large part on our continuing sponsorship of public opinion surveys conducted by Louis Harris and Associates with Dr. Alan Westin of Columbia University as academic advisor. Our 1990 landmark survey, The Equifax Report on Consumers in the Information Age, and annual follow-up surveys have revealed that most Americans are concerned about threats to their personal privacy and desire a larger degree of participation in the ways that information is gathered about them and used. The survey also found that Americans are basically pragmatic about the use of their personal financial information, value the benefits made possible by the collection and use of that information, and will support such uses as long as they know fair information practices are observed.

In a new age of technology and expanding information sources, there is clearly a need for a continuing balance between the legitimate information needs of our economic system and the privacy interests of our citizens. Current consumer protection law provides a good framework for maintaining the appropriate balance, setting out permissible purposes, establishing accuracy standards, and allowing consumers to view data and seek explanations or corrections, if necessary.

As the leading provider of information for consumer financial transactions, Equifax continues to be a pioneer in consumer-oriented initiatives, especially in the area of consumer privacy. We believe the information we gather and provide is the lubricant on which our nation's economy runs and prospers. We also believe in the rights of individuals to participate in decisions over the use of information about them: to know what information is gathered, what is done with it, who can obtain it, and what benefits accrue as a result of its proper availability.

Putting Equifax Beliefs Into Practice

THE FOLLOWING ACTIONS and initiatives have been undertaken to enhance privacy protection, improve information accuracy, and provide professional service to consumers.

- We conduct annual national surveys of consumer attitudes about privacy and fair information use.
- We consult with privacy experts, representatives of consumer groups and commentators about privacy concerns and data protection issues.
- We conduct regular privacy audits of our various information services. Dr. Alan Westin, Columbia University Professor of Public Law and Government and noted privacy expert, conducts these audits.
- Security systems are continually reviewed and strengthened to protect information systems.
- New state-of-the-art software logic helps ensure maximum accuracy in data input and delivery.
- Expert systems help ensure data integrity; automated systems track the progress of consumer requests for reinvestigation.
- Standardized formats and data reporting procedures improve speed and consistency of data.
- The Equifax Office of Consumer Affairs assures quality service and acts as an ombudsman for consumers.
- Equifax opened a first-of-its-kind Information Service Center in December 1991 - with excellent service standards and a service attitude that treats consumers as valued customers.
- Information consultants provide courteous and prompt disclosure and reinvestigation of questions or disputes. Automated systems deliver rapid service.
- Redesigned report formats improve consumer understanding of information.
- Periodic surveys of consumers who have obtained their credit report help us track performance and assure continued high service quality.

What's Next For Equifax?

WE ARE PLEASED with the progress that has been made, but we know there is more to be done. We continue to review our procedures and to look for ways to make our information more meaningful and our service more effective to businesses and consumers.

We know that continuing changes in technology, information use and public opinion must be monitored very closely and that we must adjust our practices whenever possible to improve information quality, accuracy, consumer service and privacy.

Our intent is to be the preferred steward of consumer information. We at Equifax pledge to conduct our business in accordance with the beliefs expressed in this document. We are committed to superior information practices worthy of the public trust.

What if I Have a Question?

PLEASE WRITE OR CALL us if you have any questions about your rights or our information practices. We will answer your inquiries or direct you to our appropriate business activity in accordance with your request.

Equifax Inc.

Corporate Public Affairs

1600 Peachtree Street, N.W.

Atlanta, Georgia 30309

(404) 885-8231

Mr. BAKER. Thank you, Mr. Chairman. Several of these initiatives have involved Dr. Westin, professor of public law at Columbia University, and we believe the leading privacy expert, certainly one of the leading privacy experts in the United States.

Dr. Westin consults with us on privacy issues. He conducts privacy audits of our various services. And when, in 1990, we sponsored a national survey on privacy, general privacy issues, entitled "Consumer in the Information Age," Dr. Westin acted as academic adviser to Louis Harris and Associates. He did so in 1991 and 1992 for our followup opinion surveys.

Well, last year, because of our growing businesses using health information, and because of the obviously growing public concern about medical record privacy, brought about by increasing uses of health care information and new automated health care systems, we decided to sponsor a major survey on health information privacy.

We certainly wanted to know what the public thinks the privacy rules of the road are and should be, rather than go ahead and make investments in new businesses and operate them in a vacuum.

The results were released last October and Dr. Westin once again acted as associate to Louis Harris in the survey planning and data analysis, so I think it's appropriate now to turn to him and ask him to brief us on the findings in his analysis.

[The prepared statement of Mr. Baker follows:]

STATEMENT OF JOHN BAKER

Senior Vice President of Equifax Inc.

Atlanta, Georgia

Hearing on

H.R. 4077, THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1994

Before the Government Operations Committee

Subcommittee on Information, Justice, Transportation and

Agriculture

of the

United States House of Representatives

Washington, D.C.

Wednesday, April 20, 1994

Mr. Chairman and members of the Subcommittee, my name is John Baker and I am a Senior Vice President of Equifax Inc. Equifax is a leading provider of decision-support information to facilitate transactions between businesses and consumers throughout the United States and Canada, the Caribbean, and Great Britain.

Established in 1899, Equifax provides services which enable millions of people to obtain such benefits as credit, insurance, employment, medical plan payment and check-cashing privileges on the basis of their individual merit. Our customers include retailers, insurance companies, public utilities, banks, hospitals, employers, government agencies, manufacturers and the large diversified financial services organizations that are such an important part of the American economy.

Traditionally, our services have mainly focused on the areas of credit and insurance underwriting. But in meeting the needs of our customers, our expertise has grown extensively into database management, decision support systems and other areas associated with the collection and maintenance of consumer information. As we continue to add value to transaction related information and develop new markets for information based solutions, our services relating to the health care field are growing rapidly. Our health information services include health plan administration and management, electronic processing of health care payment transactions, software/consulting with analytical services, health care provider credentialing systems and hospital bill audits. Many of these activities help to speed information

flow, improve standardization and reduce waste and inefficiency in health care systems.

Equifax continues to develop newer, faster, more secure ways to provide high quality information while adhering to the highest standards of fair information practices. We are committed to operate as responsible stewards of the consumer information we collect and maintain. We have attached as part of our testimony material which describes the role that we perform in connecting consumers and businesses, states our beliefs and policies about fair information uses, and explains the procedures and practices we follow to carry out our policies. Equifax intends to continue in a leadership role helping to define superior standards of information use and privacy.

Because of the growth in our own health information services and the growing public concerns about medical information privacy brought about by increased uses of health information and new automated health care systems, Equifax last year sponsored a major new survey on the specific subject of health and medical information privacy. This survey followed our three previous nationwide surveys, commissioned by Equifax and conducted by Louis Harris and Associates, which were designed to probe consumer opinion on a wide variety of privacy issues.

We appreciate the opportunity to appear before this subcommittee to highlight the

results of our 1993 Health Information Privacy Survey, copies of which have been distributed in advance to the subcommittee members, and to comment about their applicability to your proposed legislation. In response to your request, we are pleased to offer some information about what we have learned in the past year -- from the results of this survey of consumer attitudes and from our real world experiences -- regarding consumer expectations about health information privacy. We are accompanied today by the academic advisor to this survey, Dr. Alan F. Westin, Professor of Public Law and Government at Columbia University. Dr. Westin has conducted privacy audits for Equifax and provided privacy advice to our company over the past five years, and is widely regarded as a leading privacy expert in the United States. Dr. Westin has provided his analysis and interpretation within the survey document and has also summarized the findings and their implications in his separate testimony.

We applaud the Chairman's efforts in developing H.R. 4077, the Fair Health Information Practices Act of 1994. The development of this legislation is timely and vital to the progress of meaningful public dialogue about fair health information principles. Obviously, breaking new ground in drafting this first legislation for this complex subject has been a challenging task, and we commend you and your staff, especially your Chief Counsel, Mr. Robert Gellman, for the excellent work on this bill. We agree with the Chairman's statement that, "...regardless of how the health delivery and payment system is restructured, there is and will continue to be

a need for a code of fair information practices." We think it's time to get started defining the permissible purposes of use, consumer rights of access, information standards and security standards. In fact, last week on April 13, 1994, The Washington Times printed an Op-Ed commentary by our Chairman, Jack Rogers, entitled, "It's Time for Serious Legislation to Protect Medical Privacy." We need national rules of the road for health information privacy and we need them now. Your legislation is an excellent beginning.

Equifax supports federal legislation which enacts a comprehensive medical information privacy law designed to protect the confidentiality and security of the personal health information of all Americans. As you have stated, there will be many balances of societal interest to work out in any such law. This subcommittee's recognition that medical information is vitally important to the American public is confirmed by the results of our recent survey. This major survey of leaders' and consumers' attitudes regarding health information privacy was conducted between July 26 and August 26, 1993. Interviews were conducted with a cross-section of 1,000 Americans eighteen years of age and over with a leadership sample of 651 executives, professionals, and state and federal officials in the health care field.

As a clear starting point -- the American public continues to be deeply concerned about threats to personal privacy. A majority of leaders believe that Americans are

concerned about threats to the confidentiality of their medical records. A sizeable minority of the public (27%) believe that there has been improper disclosure of their medical information.

The public believes that protecting the confidentiality of people's medical records is essential. Interestingly, they place this priority even ahead of providing health insurance for those who do not currently have coverage. While there is a high trust in confidentiality practices of those providing direct care, there are concerns about how medical information is circulating in uses beyond direct care. And while the public believes that advanced computer technology will be essential in managing health care systems effectively, people are also concerned about the effects that the increasing use of computers could have on patient privacy.

Strong majorities favor the passage of laws to safeguard medical confidentiality and patient rights. Over half of the public say that comprehensive federal legislation is needed to clearly define rules for confidentiality of individual medical records. People overwhelmingly believe that any federal legislation enacted should designate all personal medical information as sensitive and impose penalties for unauthorized disclosure. They want rules spelling out who has access to medical records and what information can be obtained. They also favor legislating a right of access by individuals to their medical records and creating procedures for updating or correcting these records when appropriate. It is also important to point

out that while there is a strong sentiment among the public for new laws, over eight out of ten surveyed say it is important for companies which process medical information to have strong privacy policies.

Our survey indicates that your legislation calling for fair health information practices addresses the major concerns that most Americans have expressed about the privacy of medical information. HR 4077 takes a major step forward by defining protected health information, developing a trusteeship concept and setting forth access rights, notice requirements, and model forms. These concepts will undoubtedly shape the thinking and mind set of all parties involved with health care information and enable more precise discussions and better understanding of key issues.

It is especially helpful that the legislation takes an approach of defining rights and responsibilities rather than the ownership of information. We very much agree with your statement that "...the concept of ownership of personal information maintained by third party record keepers is not particularly useful in today's complex world." As in the processes of consumer reporting, both the record subject and record keeper have rights and responsibilities with respect to the information.

We are encouraged by the emphasis of "consumer empowerment." By

establishing access and correction rights, requiring consumer education processes, and instituting mechanisms to ensure knowing and voluntary consent, H.R. 4077 reflects the sentiments of an overwhelming majority of the American public. As you know, consumer reporting agencies have similar responsibilities under the federal Fair Credit Reporting Act for providing consumer access and procedures for information recheck and resolution in cases of disputed accuracy. This has been an important concept and one that has prompted additional voluntary steps to improve accuracy and clarity of the information and the speed of reinvestigation among the various consumer reporting agencies and data furnishers.

As a general principle, we believe strongly that record keepers should be permitted to recover the reasonable costs of disclosure, handling, and providing copies. We, therefore, are very pleased that HR 4077 authorizes health information trustees to charge fees to recover their reasonable costs of record disclosure.

Our company's experience with handling sensitive consumer information has shown that confidentiality is of primary importance; therefore, we applaud the bill's strong commitment to confidentiality and security. The requirements to maintain reasonable and appropriate security measures are supported by the survey results. Requirements for audit trails, regular training programs and warning mechanisms are especially appropriate.

Mr. Chairman, you and your subcommittee members and staff are perhaps better aware than anyone of the complexity and difficulty in developing comprehensive health record privacy legislation. Your legislation is innovative, creative and constructive. Inevitably, of course, your legislation also raises numerous issues which we believe warrant study and debate. Let me turn briefly to an identification of what we believe are some of these issues.

For the most part HR 4077 would impose the same information rules on all types of health care providers including doctors, hospitals, HMOs; most types of payors including various health benefit plans; researchers and public health agencies; and all affiliated parties, including a vast and disparate array of mostly private sector organizations that provide data processing services, auditing, outcome analyses, and utilization review. Our survey indicates that consumers possess different expectations about how various entities should handle personal information. For instance, the great majority of the public believes that health care providers are keeping their medical information confidential. They are more concerned about the handling of information by the next tier of organizations, including insurers, employers and public health agencies. People do not want medical records used for direct mail purposes or the solicitation of donations without prior approval. Likewise, almost two out of three Americans do not want medical researchers to use their records for studies without their permission. Therefore, the proposal to allow protected health information for research purposes and public health

purposes without patient consent or notice should be given wide publicity with a clear explanation of the public benefits.

Our survey findings suggest that HR 4077's similar treatment of providers, payers, health agencies, and all the various kinds of affiliates should be carefully studied and debated. There are many organizations that provide information services to health givers and payers - such as auditing, quality assessment, utilization review and outcome analysis. These are critical services to reduce cost and improve health care quality. In the work that follows the introduction of this legislation, we think there should be an outline of the various types of affiliates and affiliate relationships and the roles of the different parties - providers, payers, administrators, processors - in different information contexts. We believe that a detailed mapping of permissible access situations should be made for all participants in the health care system, and we would be pleased to lend our experience and analysis to that effort.

We think it is very necessary, as called for in HR 4077, to set standards for electronic documents and communications. We have recently testified before the House Subcommittee on Census, Statistics and Postal Personnel, chaired by Congressman Sawyer regarding HR 3137, which outlines a plan to establish information standards and procedures. As we said at that hearing, "it will be impossible for any health care plan to succeed unless there is in place an effective,

efficient and privacy sensitive information infrastructure to collect, maintain and transmit essential personal medical information." We look forward to working with the Secretary's staff and all interested parties to help define standards for electronic documents and communications, and we have attached to this testimony a copy of our comments regarding HR 3137.

We look forward to discussions with staff about several additional areas, including federal pre-emption (which we believe should be a presumption when dealing with regional or national health care information systems); the compatible use standard (which should probably be broadened to encompass uses compatible with not only the specific purpose for which the data was acquired but also the ongoing relationship between the parties); the permissible reporting of payment and collection data (which should permit reporting to certain third party agencies); and the damages and penalties in civil actions (which, hopefully, could include mechanisms for complaint and cure prior to statutory damages likely to attract significant litigation for technical violation).

These are all areas of attention that will be facilitated by the far sighted approach, terminology and mechanisms of HR 4077. We are very encouraged, Mr.Chairman, by your proposals for fair health information practices, and we believe that as they are examined and debated, they will encourage new approaches in the marketplace for the protective handling of health record information. Final legislation will want

to take into account marketplace self-regulatory developments and include a degree of flexibility so that innovative and practical approaches that result in privacy protection and fair practice, as determined by the Secretary or review boards, can be accommodated.

We are encouraged by this Subcommittee's willingness to address the complicated issue of health information privacy. Equifax is committed to participating in the effort to establish and maintain a delicate relationship between the legitimate information needs of health care organizations, the needs of society and the right to privacy. We appreciate the opportunity to testify today, and look forward to working closely with you and this subcommittee and other interested parties in the discussion of fair health information practices.

It's time for serious legislation to protect medical privacy

By C.B. Rogers Jr.

Now that serious attention is being given to developing a health care reform program, I believe that Congress should enact a comprehensive medical information privacy law to protect the confidentiality and security of the personal health information of all Americans. I believe Congress must do this now, not three years after a national health reform plan is enacted, as originally proposed by the Clinton administration.

Federal action is needed for two fundamental reasons:

First, health industry leaders and the public see federal action as a priority in reshaping the nation's health care system. Last year, Equifax sponsored an in-depth national survey by the Louis Harris organization and Dr. Alan Westin of Columbia University, one of the nation's leading privacy experts. The survey found:

- 85 percent of the public and similar percentages of health industry leaders rank "insuring the confidentiality of people's medical records" in any health care reform as "very important" or "absolutely essential."

- 27 percent of the public — representing 50 million American adults, report that an organization to which they have given their medical information has disclosed it to others improperly. Fifty-nine percent of health industry leaders say they consider violations of medical record confidentiality "a serious problem" today.

- The lack of legal guidelines for handling personal medical information beyond the places where direct health care is provided worries both the public and industry. That is why, even though laws defining medical privacy have tradition-

ally been set at the state level, 56 percent of the public and 65 percent of hospital leaders told the Harris interviewers that the time has come for rules on health information confidentiality to be set on a national basis.

The second reason we need national privacy standards is to guide the operations of computer systems that are increasingly being used to automate patient records and provide electronic health data exchanges. Information-technology firms such as Equifax know that electronic systems will be vital to improving patient care, reducing paperwork burdens, controlling health-system costs, and fighting fraud. The American public agrees:

- 76 percent believe it will be essential to increase individual record-keeping and apply advanced computer technology "if we are to manage health care reform efficiently."

- 84 percent say it is acceptable to issue everyone a national health insurance card for accurate identification and to administer a national health care system.

But the public is also concerned about the effects that increased computer uses could have on patient privacy. Three out of four worry that medical information in a computerized national health information system will be used for many non-health purposes, and 75 percent worry that persons inside the health care system may disclose information improperly.

The bottom line is that the public wants the benefits of technology applications in health care — and health care reform — but is worried about the way that personal medical information is being handled today. People want enforceable rules of the road from Congress.

Unlike some privacy situations in recent years — where business or government agencies disagree with consumer and privacy advocates about the content of federal regulation — the leading players in health care privacy have been moving toward a basic consensus during the past year. The key principles of a national health information privacy law have been well identified — and drew very strong public support when they were tested in the Harris survey. A good statute should:

- Designate all personal medical information as sensitive and penalize unauthorized disclosure (sup-

The bottom line is that the public wants the benefits of technology applications in health care — and health care reform — but is worried about the way that personal medical information is being handled today.

ported by 96 percent of the public).

- Spill out who has access to medical records and what information can be obtained (supported by 96 percent of the public).

- Provide a right of access by individuals to their medical records in the system. This not a legal right today in 23 states (supported by 95 percent of the public).

- Encourage selection of data processing organizations handling personal medical information based on their record of implementing confidentiality and security standards (94 percent of the public agrees).

There will clearly be many balances of social interest to work out in any such law. But the time to develop and refine a national health information privacy law has come. As a company already involved in handling health measurement and health claims data, we have our own code of privacy and fair information practices for handling medical records. But we, like the health care professionals and health care support industries, need the standards of a sound national law to guide our relationships with each other and with all the individuals whose records are entrusted to us.

The message is clear: No health care reform plan will be acceptable to the American public unless the privacy, confidentiality, access, and security issues involved in a national health care system are directly and comprehensively addressed by federal legislation.

The Washington Times

WEDNESDAY, APRIL 13, 1994

Reprinted with permission of The Washington Times

Mr. CONDIT. Dr. Westin.

STATEMENT OF ALAN WESTIN, PROFESSOR OF PUBLIC LAW AND GOVERNMENT, COLUMBIA UNIVERSITY, NEW YORK, NY

Dr. WESTIN. Mr. Chairman, Ms. Woolsey, I've been working on surveys of the public attitudes on privacy now for about 15 years. At my latest count, I think it's been about eight national major surveys and perhaps a dozen special topic surveys.

And I think what's distinctive about this one are two things. First of all, the way in which the results have been embraced, I think is the fair term, by all of the sectors that are wrestling with these issues; that is, industry, public interest and advocacy groups, government people who regulate and oversee the health care system, and even academic survey experts.

The survey has been well received as having asked the right kind of questions generally, in the right way, and produced data that is insightful as to not only what the public thinks of values and experiences, but also, since we knew a bill like this was coming down the pike, what are the principles of a Federal bill that the public could be asked about and express an opinion on.

The second element of the survey is that we not only did a public survey of 1,000 respondents of 18 years of age and older representing the national population, but also of 651 leaders, divided among the health care industry—heads of HMOs and hospitals and health insurance executives, of government officials, legislators and regulators who deal with health affairs, and doctors, nurses, care deliverers, and also employers representing the human resources function inside the employment area.

And unlike some situations in which you get some gap, if not a complete conflict between the views of "an industry" and consumer and privacy advocates on the other hand, here we found a striking congruence between the concerns and the policy attitudes on the part of the general public, on the part of a particularly interested segment of the public and the leadership in all of the areas that I mentioned.

With that in mind, let me suggest five top-line findings that I think are the most important ones in terms of H.R. 4077 and the whole legislative process you're engaged in.

First of all, a remarkable 27 percent of the public, which represents about 50 million American adults, reported to us that they believe that an organization or a person that they had given their medical information to willingly and were using it for the right purpose had disclosed it in ways that the respondent thought was improper.

So we have 50 million Americans who report an experience that they believe that their medical information was disclosed in ways they thought were inappropriate.

Since paranoia is not unknown on the part of the public, we tried to test that by asking the health leaders themselves what they thought about improper disclosure, and found again, a rather dramatic parallelism, that 24 percent of the health and government leaders that we asked, "Do you know of an instance, an episode in which medical information was released improperly?" reported the very same fact, and they documented for us in ways that the sur-

vey report lays out specifically who was doing the disclosure and what kind of injury was done to people.

And I think our data are very clear and very helpful, I would hope, to this committee in suggesting that for tens of millions of Americans, the feeling is that their employment opportunities or their insurance opportunities or their reputations and feelings of security in the handling of their personal medical information were compromised because of weak rules, absence of safeguards, et cetera.

And the conclusion that we got from the health leaders and the government leaders was that 59 percent of them, when asked, said that they considered violations of medical record confidentiality to be a serious problem today. And when you get leaders classifying something as a serious problem, when they're quite capable of saying it's only a minor problem or it's not really a problem, I think that's a very important element to factor in.

Second, we asked the public how important assuring the confidentiality of people's medical records was to national health care reform. We gave them a list of seven or eight objectives of national health care reform, and 85 percent of the American public listed protecting the confidentiality of people's medical records in national health care reform to be absolutely essential or very important.

And they put this ahead of such sterling objectives of national health insurance reform as providing health insurance for those who don't have it today, reducing paperwork burdens on patients and providers, and obtaining better data for medical research. So even such important and laudable objectives, in the minds of the public, did not keep up with or match the intensity of feeling on the part of the public about assuring confidentiality in national health care reform.

The third major finding is that Americans clearly accept the fact that individual recordkeeping will have to be increased, that advanced computer technology will have to be invoked and applied if we're going to manage health care reform efficiently. Seventy-six percent of the public, three out of four Americans, signed on to that kind of an expectation and statement.

And when we asked specifically about the national health insurance card for accurate identification and to administer the system, 84 percent of the public said that they thought that such a national health insurance card was acceptable.

However, and this is where the kind of problems of interpretation and of judgment on the part of the public coincide with what is clearly the same feeling of concern and some indecision on the part of policymakers, we went on to ask about how people felt on having an identification number for the health insurance system, and 57 percent of the public said that they would be concerned if everyone were assigned an identification number, in itself.

However, they were asked if a number was issued, would they prefer to have the Social Security number used or a new national health identification number, and 67 percent, two out of three, said they'd prefer to have their existing Social Security number used.

On the one hand, I think that may be a convenience response, that I know my number; I don't want to have to remember another number. Second, I don't think it probably reflected the kind of

thinking process that might arise when people were brought to an awareness of some of the problems of linkages and of misuse of the Social Security number.

So I don't think that one should take that reading as a kind of definitive last judgment about Social Security number versus other numbers. I think that is going to have to unfold as the discussion and debate about various kinds of alternative identifiers, biometric identifiers, PIN numbers, Social Security numbers plus, and a variety of other solutions may come up.

Finally in these top-line findings, we asked whether people felt that it was important that individuals have the legal right to obtain a copy of their own medical records, which is not the case in about 23 States today, and the public was virtually unanimous, 96 percent believing that that kind of legal right was something that should be enacted in any contemporary medical information system.

Then we asked whether people believe that comprehensive Federal legislation was needed or whether we should leave this to the States and current practice, and 56 percent of the public and 58 percent of leaders believe that comprehensive Federal legislation is needed to spell out rules for confidentiality of individual medical records in any national health care reform system.

And again, we know from much survey research that Equifax and Louis Harris have sponsored in the last 4 years that the public is quite capable of saying no to Federal regulation if they don't believe that this is necessary, and therefore, this kind of endorsement, I think, is a significant finding for the work of this committee.

Let me shift now to a couple of additional matters that I think are worth mentioning before trying to analyze and sum up what I take to be the major thrust of the survey findings for the particular piece of legislation here.

It's clear that the public, as our earlier surveys have found, is capable of discriminating between those uses of information that they think provide high social benefits and is relevant for decisionmaking. And so the survey found that, for example, the public approves of life insurance companies asking questions about medical history and about alcohol and smoking and other kinds of relevant factors in deciding whether to issue a life insurance policy or what rate to set for it.

In addition, it's seen on the part of the various people that they don't want uses made of their medical information where they do not have the right kind of notice and consent. So, for example, 60 percent believe that it's not acceptable for pharmacists to provide medical information about them without their individual approval to direct marketers who may want to mail them offers of new medications or new medical devices for particular conditions.

And in the finding that Ms. Hunter alluded to, we found that almost two out of three respondents, 64 percent, don't want medical researchers to use their records for studies, even if they're never personally identified, unless those researchers first get the individual's consent.

Now, I think that it's going to be important to spell out some additional questions for the public on what the conditions are that

would make people more comfortable with important research uses being made of their records, and I hope we'll be able to do that.

Turning to national health legislation, we took some of the concepts that wound up in H.R. 4077 and put them as questions to the public about what they thought should be in any national health legislation fair information practices legislation.

Ninety-six percent of the public believe any Federal legislation should designate all personal medical information as sensitive and impose penalties for unauthorized disclosure. A similar 96 percent support rules that would spell out who has access to medical records and what information can be obtained.

Ninety-five percent favor legislating a right of access by individuals to their medical records in the system and creating procedures for updating or correcting such records.

And finally, 86 percent of the public favor creating an independent national medical privacy board to hold hearings, issue regulations and enforce standards.

If you look at the survey, you'll see that behind those very large numbers, in the 90 percents, we asked about what was absolutely necessary and what was important, and so you can see that some of these scored much more highly as being absolutely necessary, but the total numbers show very strong agreement on the part of people as to what should be in this kind of legislation.

One other point that I thought was interesting is that when asked about how information processing companies should be chosen in order to do analysis of treatments, results and costs, 94 percent of the public believe that companies should be selected on the basis of a proven record of protecting the confidentiality and security of the personal records they handle.

Let me draw back now and make a few analytic points, if I may.

Mr. CONDIT. Dr. Westin, we've got about 6, 7 minutes to go cast a vote. Can both of you stay?

Dr. WESTIN. Yes, we can.

Mr. CONDIT. We'll return in 10 minutes or so and let you conclude your remarks, and then we have some questions for you. Thank you.

[Recess taken.]

Mr. CONDIT. Maybe we can get going.

We apologize to both of you and to the audience. We had two consecutive votes and probably we'll start voting here again in the next 20 or 30 minutes. So Dr. Westin, we'll let you conclude your remarks, then try to wrap up our questions, and if we don't get to all our questions, maybe we can submit those to you in writing.

Dr. WESTIN. Thank you very much. I was about to say that sometimes when you do surveys and you look at the answers to particular questions, you really ask yourself, what does it all add up to in terms of consistency of viewpoint on the part of the public and also intensity of viewpoint on the part of the public. There's a tendency to do policy wonk questions to the public in which you get answers back but you're not really very sure about where the attitudes are coming from.

We found in this survey that almost half the public, 48 percent, when you analyze their answers to about 39 or 40 of the questions

on the survey, reflected what could be called intensive concern about medical record confidentiality and privacy.

The way we came up with that figure was to look at those respondents who reported that they or their immediate family members have used mental health services—that's about 22 percent of the population, and they are very, very concerned about the sensitivity of medical information. Twenty-seven percent of the public, as I mentioned, who reported that their personal medical information, they felt, had been disclosed improperly.

And then finally, we had a sensitivity index of people who are especially concerned about misuse of computers and also about potential misuses of their medical information in a high technology environment.

And when we eliminated duplicates in those three groups, that's where we came up with the 48 percent of people who, on the substantive questions on the survey, scored high in a strong majority of the questions that we asked.

That represents about 89 million Americans. And I think that that, Mr. Chairman and members of the committee, is your constituency. Those are the Americans who are mobilizable for this bill, who can be energized by the right kind of publicity and by the right kind of collection of episodes and stories that illustrate how people's privacy rights can be trampled on, and that in this kind of a setting, if the word can get out to those kinds of people, 48 percent of the population, you have the wherewithal for strong support for congressional action.

What's interesting is that group combines two interesting subsets of the population. Part of them are from high income and high status portions of the population—people who use mental health services and report breaches of confidentiality—but they're joined by almost half of that number, low income, minority, and senior citizens groups, who scored the highest on our sensitivity index.

So it's a very interesting combination of elements in the population that share this common concern about medical sensitivity.

Let me conclude by saying that I think there's one message that the survey sends clearly to the Clinton administration, to Congress, to health leaders and to all the interest groups, and that is that the American public is not very trustful at the moment of institutions that want to reassure them that their health information will not be misused.

They're going to be looking to concrete action on the part of Congress and on the part of administrators and on the part of all the groups that are involved in processing medical information, private sector companies and the professions themselves.

What they want, and I think H.R. 4077 responds quite directly to the issues that were raised and tested in the survey, is to have a system of rules, to have meaningful safeguards and remedies, and to give private rights of action for people so that they feel that they're not dependent always on what others will do on their behalf.

And it's that combination of rules and remedies and initiatives that I think the American public will want if they are to feel that their confidentiality of information is to be protected.

I think this is an excellent bill, one that gets us started in exactly the right direction. I'd be delighted to work with you on the details of it, and I think the Equifax survey of 1993 shows that you're responding to an extraordinarily sensitive issue for the majority of the American public and properly mobilized, they will be behind you with it.

[The prepared statement of Dr. Westin follows:]

**Testimony of Dr. Alan F. Westin, Professor
of Public Law and Government, Columbia
University**

**on the Fair Health Information Practices Act of
1994 (H.R. 4077)**

**before the Government Information, Justice,
and Agriculture Subcommittee of the Committee
on Government Operations**

Washington, D.C., April 20, 1994

Background

Chairman Condit and Subcommittee Members, I am very pleased to testify today at these important hearings on federal protection of individual privacy in the handling of health information and medical records. As a professor at Columbia University and an expert on privacy, I have been concerned about privacy of medical and health information for three decades.

In the 1960's, I looked at the uses of medical information during the early days of computerization (Privacy and Freedom, 1967). Between 1974-1976, I directed a study for the U.S. National Bureau of Standards that mapped in detail how personal medical records and health information were flowing out of direct care into payment and review sectors, and into the larger zone of social uses of medical information. (Computers, Health Records, and Citizen Rights, 1976.) Since 1978, I have led a series of public opinion studies on privacy as academic advisor to Louis Harris & Associates, with a frequent focus on how Americans feel about handling of their personal health information. (A short bio of my health-privacy activities appears at the end of this statement.)

I am also the publisher of Privacy & American Business, a new, non-profit national bi-monthly report on key privacy issues affecting all American businesses that rely on uses of personal information about their customers, clients, employees, patients, and other individuals with whom they have -- or hope to have -- business relationships. Privacy & American Business devoted the In Depth section of its second issue (in early 1994) to the health information privacy issues and national health care reform. We not only reported in detail on the national survey I will be describing today but we also described the landscape of organizational activities and supporting studies, codes, and public expressions that demonstrate converging concerns policy on the need for health privacy legislative action by Congress.

(I have included a copy of this In Depth section of Privacy & American Business with my prepared statement, for inclusion in the hearing record)

The Harris/Equifax Health Information Privacy Survey, 1993

Today, I appear at your invitation to relate the major findings of a national survey on "Health Information Privacy" conducted in 1993 by Louis Harris & Associates, sponsored by Equifax Inc. The Equifax survey is the most comprehensive and detailed study yet conducted of the American public's experiences, attitudes, and concerns over the handling of their health information, particularly in the context of national health care reform, as well as the views of health industry and government leaders.*

These findings confirm the urgency with which both large majorities of Americans and large majorities of health care leaders favor the enactment of federal legislation to define and protect health-information privacy rights. The findings also support strongly many of the particular approaches of H.R. 4077, the Fair Health Information Practices Act of 1994.

First, let me summarize what I see as five of the most relevant findings of the survey for.

FIVE TOP LINE FINDINGS

1. Improper release of medical information

A remarkable 27% of the public -- representing 50 million American adults -- believe that an organization or person legitimately having their individual medical information has disclosed it improperly. Twenty-four percent of health and government leaders parallel the public's response, reporting that they personally know of such improper disclosures of medical information. Overall, 59% of leaders say that they consider violations of medical record confidentiality to be "a serious problem" today.

2. The critical importance of confidentiality in health care reform

Eighty five percent of the public say that protecting the confidentiality of people's medical records is "absolutely essential" or "very important" in national health care reform. They

* The Harris/Equifax survey polled a representative public sample of 1,000 persons 18 years of age or older. Some 90 substantive questions were posed, along with standard demographic data. In addition, 651 leaders were polled, drawn from the communities of health care and supporting services, government officials dealing with health issues, and employers. The surveys were administered in July-August, 1993. The full report, The Health Information Privacy Survey, 1993, is a 153-page document and single copies are available without charge by writing to the Public Affairs Department, Equifax Inc., 1600 Peachtree Street, Atlanta, Georgia 30309

The survey findings were issued publicly on October 29, 1993, at a national Health Information Privacy Conference in Washington, D.C. The conference -- attended by over 200 health industry representatives, government experts, and public-interest group representatives -- was co-sponsored by the American Health Information Management Association and Equifax, in cooperation with the United States Office of Consumer Affairs.

put this priority even ahead of reform goals such as providing health insurance for those who do not have it, reducing paperwork burdens on patients and providers, and obtaining better data for medical research.

3. Support for record-keeping and health cards

Seventy six per cent of American adults believe that individual-record-keeping will have to be increased and advanced computer technology applied to manage health care reform efficiently. Eighty four per cent say it is acceptable to issue everyone a national health insurance card for accurate identification and to administer the system.

4. Concerns over computers and identity numbers

However, 75% of the public worry that medical information from a computerized national health information system will be used for many non-health purposes. And 57% would be concerned if everyone were assigned an identification number for the health insurance system. But if a number is issued, 67% would prefer using their existing Social Security number to having a new national number just for health insurance.

5. Strong support for privacy and access laws, and a federal standard

The public is virtually unanimous -- 96% -- in saying it is important that individuals have the legal right to obtain a copy of their own medical records (not the law today in 23 states). Fifty six percent of the public and 58% of leaders say that comprehensive federal legislation is needed to "spell out rules for confidentiality of individual medical records" in national health care reform; they reject relying on current laws and organizational practices.

OTHER MAJOR FINDINGS

Some other findings of the Harris/Equifax survey relevant to these hearings are the following:

- **trust in care providers**

Eighty seven percent of the public in 1993 believes the health providers they use are doing a good job in keeping their medical information confidential. Only very small percentages cite any health service providers -- doctors, hospitals, or pharmacists -- when listing organizations they believe have disclosed their personal medical information improperly.

- **provider use of computers**

Reflecting high general fears about computer handling of personal information, half the public (50%) say they are concerned that their health care providers are using computers today in managing accounting and lab work and keeping medical records. Strong majorities worry that this computer use may cause mistakes in charges (75%); mistakes in medical conditions put into patient records (60%); and medical information being given to people who aren't supposed to see it (64%).

- **worries about how medical information circulates**

Forty one per cent are worried that medical claims information submitted under an employer health plan may be seen by their employer and used to affect their job opportunities. Sixty per cent believe it is not acceptable for pharmacists to provide medical information about them -- without their individual approval -- to direct marketers who want to mail them offers of new medications. Almost two out of three (64%) don't want medical researchers to use their records for studies, even if they are never identified personally, unless such researchers first get the individual's consent.

- **social uses of health information**

The public approves of relevant and proper uses of medical information beyond the direct care setting. For example, large majorities -- from 62-81% -- say it is acceptable for life insurance companies to collect medical or health-related information to decide whether to issue a policy and at what rate. Acceptable information includes whether applicants drink alcohol, smoke tobacco products, or engage in dangerous sports; the applicant's medical history of past diseases and illnesses; and the applicant's family history of inheritable conditions. The public also believes it is acceptable for life insurers to require urine tests to detect illegal drugs and blood tests for AIDS or the HIV virus.

- **national health privacy legislation.**

Ninety six per cent of the public believe any federal legislation should designate all personal medical information as sensitive and impose penalties for unauthorized disclosure. A similar 96% support rules spelling out who has access to medical records and what information can be obtained. Ninety five per cent favor legislating a right of access by individuals to their medical records in the system, and creating procedures for updating or correcting such records. Finally, 86% of the public favor creating an "independent National Medical Privacy Board to hold hearings, issue regulations, and enforce standards."

- **information-processing companies and privacy**

Ninety-four per cent of the public say that information-processing companies hired to review individual medical records for analysis of treatments, results, and costs should be selected "on the basis of a proven record of protecting the confidentiality and security of the personal records they handle."

Almost Half the Public Register Very High Concern

Looking into underlying sources of these attitudes -- stemming from medical conditions, experiences with breaches of medical confidentiality, and deeper social attitudes -- the survey identified three subsets of the population that adopted consistently strong privacy positions on a majority of 39 substantive questions the survey presented about medical privacy.

- respondents who report they or immediate family members have used mental health services (22%);
- respondents who report that their personal medical information has been disclosed improperly (27%); and
- respondents who score high on a "sensitivity index" measuring a combination of strong fears over computer uses and worries about potential misuses of medical information (13%).

After eliminating duplicate appearances across the three groups, the survey found that 48% of the American population -- ~~representing about 89 million Americans~~ -- display consistently strong medical privacy concerns.

What is significant is that this 48% of the population combines people from the high-income and high-status portion of the population (those using mental health services and reporting breaches of confidentiality) with people of low-income, minority, and senior-citizen status (scoring highest on the sensitivity index).

Public and Leaders Compared

The survey's sample of 651 Leaders was drawn from three groups: (1) leaders from health services (hospital, HMO, and health insurance senior executives; physicians; nurses; and medical society executives); (2) government officials (state and federal legislators and regulatory officials concerned with health affairs); and (3) employers (represented by senior human resources executives.)

Unlike the results of surveys in other business sectors -- where industry leaders often register significantly less concern about privacy and less support for privacy protection measures than the public -- the 1993 Harris/Equifax survey found health services leaders and employers to hold privacy attitudes very similar to those of the public. Industry leaders were either more

privacy-oriented than the public or about the same on almost two-thirds of the 24 key attitude and policy questions asked of both leaders and the public.

However, leaders are *more* pessimistic about protection of privacy in health care reform than the public is. While 54% of the public feels that privacy of medical records will probably be better protected in health care reform than it is today, only 23% of leaders think that will probably happen. And, in a question asked only of the leaders, a bare 50% said that they felt increased computerization of medical and health records "could be managed to help strengthen the confidentiality of such records," while 45% felt computerization "is almost certain to weaken confidentiality." (5% had no opinion)

Fortunately, the survey shows there is broad agreement between the public and leaders on both the crucial importance of legislative privacy action and on the basic measures that are needed. Whatever their differences on other aspects of health care reform, health-care providers, insurers, medical society leaders, employers, and government officials overseeing health care share the public's concerns over medical privacy.

What The Survey Warns About Health Care Reform

The survey contains a clear warning to the Clinton Administration, Congress, the health-industry, and interest groups concerned with health care reform. The American public supports the need for health care reform and also the need for applications of advanced technology to administer it well. But the public also wants medical confidentiality and patient-access rights to be clearly and strongly protected in any reform system adopted.

As the debates unfold over coverage, costs, consumer choice, local options, and Federal Government roles, the American public will be looking for a detailed federal code of fair health information practices, with the kinds of specific guarantees and mechanisms that majorities in the 80-96% range favored when presented with these on the survey.

This Bill Is In Direct Line with Major National Public Concerns and Policy Preferences

I am pleased to note that this is the approach that H.R. 4077 adopts, placing it in direct and meaningful response to the concerns registered by the Harris/Equifax survey. You deserve much praise, Mr. Chairman, for developing and presenting this bill. The results of the survey indicate that large majorities of the American public and of health care leaders should be ready to support you.

I also applaud the wide consultation process by which the Committee's staff expert, Robert Gellman, has constructed H.R. 4077. While there will surely be improvements and refinements of this initial draft – and I will be happy to work with the Subcommittee in this

Bio of Professor Alan F. Westin in the area of privacy and health information

General

Alan F. Westin is Professor of Public Law and Government at Columbia University, where he has taught for the past 34 years. Born in 1929, he earned his B.A. from the University of Florida; his LL.B. from Harvard Law School; and his Ph.D. in political science from Harvard University. He is a member of the District of Columbia Bar, and is listed in Who's Who in America.

Privacy Overall

For four decades, Professor Westin has specialized in studying, writing and consulting about the social, ethical, and legal impacts of information technology on individuals, organizations, and society. His award-winning 1967 book, Privacy and Freedom, is considered the leading work in this field. Other books he has written about privacy include: Databanks in a Free Society (1972), with Michael Baker, for the National Academy of Sciences, and two monographs for the U.S. National Bureau of Standards on Computers, Health Records, and Citizen Rights (1976) and Computers, Personnel Administration, and Citizen Rights (1979). He is currently completing a new book for the Columbia University Press on The American Public and Privacy: New Roles and Rules for the Computer Age.

In the governmental arena, he was a consultant to Senator Sam Ervin Jr. in drafting the Federal Privacy Act of 1974; a Presidential appointee to the National Wiretapping Commission (1973-76); Senior Consultant to the U.S. Privacy Protection Commission (1975-77); and a member of Privacy Task Forces for the U.S. Department of Commerce, General Services Administration, Social Security Administration, and other federal Agencies. He has been chair or a member of a dozen panels of the U.S. Office of Technology Assessment on privacy issues over the past two decades, and has testified frequently since the late 1950's before congressional and state legislative committees on privacy issues involving credit, employment, medical and health records, banking, insurance, law enforcement, telecommunications, and other issues.

In the private sector, he has been a consultant on privacy to corporations such as Citicorp, IBM, Security Pacific National Bank, Equifax, Prudential, Aema Life & Casualty, Bell Atlantic, Chrysler, and American Express; served as Chair of the American Civil Liberties Union's Privacy Committee; and directed the National Academy of Science's Project on Computer Databanks.

In addition to writing for law reviews and scholarly journals, his articles on privacy issues have appeared in the New York Times, Wall Street Journal, Fortune, Business Week, the Los Angeles Times, Newsday, the New Republic, and many other general publications. He has discussed privacy issues on the Today Show, CBS Morning Show, the McNeil-Lehrer Show, and many others.

Over the past 15 years, he has been the academic advisor to Louis Harris & Associates for the leading national public opinion and leadership-opinion surveys of privacy conducted in the United States and Canada. These have included national surveys on "The Dimensions of Privacy" (for Sentry Insurance, 1979); "Consumers in the Information Age" (for Equifax, 1990); "Updates on Consumer Privacy" (1991 and 1992); "Consumers and Privacy in the Information Age" (for Equifax Canada, 1993); and many proprietary privacy surveys for business firms and industry associations.

endeavor – this is a strikingly excellent initial bill, a fact that bodes well for its ultimate passage in Congress.

In 1993, Dr. Westin founded and serves as Publisher of Privacy & American Business, a non-profit, bi-monthly report and information service covering key issues of privacy affecting all businesses that use personal information about customers, employees, and potential customers.

Privacy and Health Information

Since the mid-1960's, Professor Westin has maintained a continuing special interest in medical confidentiality and health-information-systems privacy issues.

A comprehensive field study of computerization trends and health information was led by Dr. Westin for the U.S. National Bureau of Standards between 1974-76, and produced Westin's report on Computers, Health Records, and Citizen Rights (1976). The Privacy Code this report recommended was sent by NBS to every hospital in the U.S., and served as a model for hundreds of hospital and health institutions. The NBS Report remains to this day the leading empirical study of how computer use is affecting the three main zones of health information use -- direct care, payment and quality-assurance, and social uses of medical data.

Between 1978 and the early 1980's, he served as Research Director of the National Commission on Confidentiality of Health Records, a national association composed of the major health-care provider, payer, and quality-care associations in the United States. During this period, he spoke frequently on privacy and health information issues at national conventions or special meetings of the American Medical Association, Health Insurance Association, American Medical Records Association, American Orthopsychiatric Association, American Psychiatric Association, and many other health-professional groups.

In the past 2-3 years, he has been a feature speaker at the U.S. Department of Health and Human Services Privacy Task Force Conference on Medical Records and Privacy (February, 1993); a reviewer of reports on privacy for the National Institute of Medicine (on emerging regional health data systems), the Journal of the American Medical Association, and for the U.S. Office of Technology Assessment (on privacy and the computerized medical record).

Dr. Westin is the privacy advisor to a forthcoming Public Television Special Documentary on "Privacy and Health in the American Workplace." Dr. Westin drafted a national corporate-employee and human resources executives survey conducted by Louis Harris and Associates for use on this program, covering employee health and privacy issues in depth.

In 1993, he served as the academic advisor for a national public and leaders Harris survey on "Health Information Privacy." Results from this survey were released at a national conference in Washington, D.C. in November, 1993, at which Dr. Westin spoke, co-sponsored by the U.S. Office of Consumer Affairs, the American Health Information Management Association, and Equifax Inc.

Also in 1993-94, Dr. Westin is serving as Principal Investigator on a 15-month project on social science studies of privacy relevant to uses of genetic testing and genetic-test applications, funded by the U.S. Department of Energy for the Human Genome Project and its ELSI Program (Ethical, Legal and Social Issues).

Mr. CONDIT. Thank you, Dr. Westin. We appreciate your testimony. We appreciate your patience and your being here this morning.

Mr. Baker, did you want to summarize or close?

Mr. BAKER. Yes, sir, if I could take another minute or two.

Mr. Chairman, Ms. Woolsey, Mr. Horn, the op-ed commentary that I referred to earlier from last week, in that commentary we said that legislation should really do a number of things: designate medical information as sensitive, penalize unauthorized use, spell out who has access under what circumstances, provide a right of patient access, and encourage confidentiality and security practices. I believe that your bill really addresses these issues.

If I might just state a few things that we're in complete support on, we like the approach of defining rights and responsibilities of the parties, rather than trying to get into who owns what, which we think is less useful, as you have said. We think there are meaningful consent mechanisms set up by the bill that give consumers access. They allow recordkeepers to charge their reasonable costs, which we think is proper.

The definition of protected health information does exclude data that does not identify the individual, so it wouldn't appear to restrict the uses of aggregate data for outcome evaluation, cost-benefit statistics. And even where there is identification, and it's a protected health information, the disclosure is permitted for important research uses.

And we've had a lot of discussion about the survey and the public concern about that and the speculation, I believe, by Nan Hunter that if the questions were more properly or more deeply worded, they might elicit, with more information about the benefits of public health services and research, a more acceptable response on the part of the public, and I think that may be something worth pursuing.

With regard to the issue of permissible uses and who has access to information under what circumstances, and I think this might be our chief observation, there are many different entities with different data uses, all with the same rights and duties under the label of health use trustees or affiliated persons—doctors, HMOs, review companies, processors, insurers, health plans, and so forth.

And we think it might be useful and helpful to add more precision, so that each participant's role is described or charted with the duties and rights defined for the various information uses that they make.

It seems likely to us that perhaps some trustees and affiliates should have different rights and responsibilities than others, and I'd just like to say, Mr. Chairman, that attending this meeting this morning with me from Equifax is Jim Perkins, seated behind me, a senior vice president in charge of our health information companies, and certainly he and his staff would be pleased to work with the subcommittee in mapping out some of these various information uses and purposes.

We think that effort would be worthwhile because we know from our surveys that the public wants to make the call for different information use situations, as to where the appropriate privacy boundaries lie.

Mr. Chairman, you realize more than we do how complex and difficult it is to develop comprehensive health privacy legislation. We think your bill is creative and constructive, with a number of approaches and concepts that we believe will shape the future thinking about these issues for the time to come.

The areas that have been discussed, I'll just highlight some areas that we talk about in our testimony, without really much comment. Federal preemption—we think that's important, particularly, as Ms. Hunter said, in the area of transaction processing, payment mechanisms. That should be very strong, we think.

The compatible use concept we think is a very good concept, one that perhaps might be expanded to include those uses that people normally and reasonably would expect to occur in an ongoing relationship between the particular parties.

Identification systems we've talked about. It seems imperative that there be some identification system to achieve accuracy, efficiency and eliminate fraud. The task will be to build in proper limitations on the use of that identification and on the linkages that can be made with those identifiers and other information systems.

I think this bill will encourage companies to develop voluntary fair practices and that final legislation may want to recognize some of those and be drawn flexibly enough to incorporate suitable ones in the overall legislative package.

Again, Mr. Chairman, we'd like to compliment you, the committee members, your staff for this excellent start, defining proper fair health information practices. We think your approach, from our survey, is in synch with public opinion, and we look forward to working with you and the staff and the committee members on it.

Mr. CONDIT. Thank you, Mr. Baker. Thank you for your help.

I've got a couple of questions. I have a couple of pages of questions, but I'm going to maybe submit those to you and let you respond in writing. But maybe I'll just ask a couple of them and then defer to my colleagues.

The polls show that most people, at least 87 percent, believe that health providers do a good job in keeping information confidential. Do people really have a good basis for this belief? Can they really tell whether the hospitals really protect them or not?

Dr. WESTIN. Well, I read the figure this way, that most people, in their experience with the direct health care provider, certainly if it's the physician or the therapist, view that person as trying to give them vital and necessary treatment and wanting to keep as much confidentiality in that one-to-one relationship.

But they also appreciate that to get paid for that service, the professional may have to disclose some thing, and that worries some patients, but generally they hear their own doctor or hospital personnel say that they're also concerned about diagnoses that would be misunderstood.

So I think on the whole, the public, our survey shows, is highly trusting of the direct people that are helping them. It's really when it gets outside the treatment setting and is released under various requirements of reporting or financing or other kinds of issues that the public begins to feel nervous.

Mr. CONDIT. So I take it that they have confidence, and rightly so, in the hospital infrastructure, but maybe outside that?

Dr. WESTIN. They get nervous when the insurance function comes in, when they worry about who's looking at their record for payor, quality care assurance and so forth. They want to be reassured that in those setting, the right people are looking at it and that it's not being used, especially then in the employment relationship or in something else that will limit their opportunities.

Mr. CONDIT. Mr. Baker, Equifax is a credit bureau.

Mr. BAKER. Yes, sir.

Mr. CONDIT. But it engages in other businesses that involve the use of health information. Is there a strict functional separation between health claims processing information and other consumer information obtained by Equifax? How is that separation enforced?

Mr. BAKER. Yes, sir. I think the best answer is that it's a separation as a matter of principle, practice. It's separated as a matter of privacy and relevancy, and it's also separated as a matter of law in that there are regulations that set permissible use requirements on consumer reporting information, which therefore has to be kept separate.

Structurally it's enforced by actual structural separation—separate data bases, separate computers and so forth.

Mr. CONDIT. Thank you. Mr. Horn.

Mr. HORN. Thank you, Mr. Chairman. I'm sorry we had to go to the floor to have these votes, and you might have well covered some of these in your testimony.

I'm a long-time advocate of a fool proof, counterfeit proof Social Security card, and I've heard all the arguments that have been made by some of the original designers of the system, that that number was not supposed to be used for any other purpose but Social Security.

Reality is it is used for almost every purpose where identification is needed in our society. Universities are a prize example. Most of the registration records in my former institution, and I suspect Columbia, but I'm not positive, are tied to a Social Security identification number and when you don't have one, the university then makes up a number to somehow identify this James Smith from that James Smith.

What I'm curious is in your study, you state that most people would prefer to have their Social Security number used rather than a separate health insurance number. How was this question phrased and do the respondents understand that the Social Security number can be linked to other personal documents?

Dr. WESTIN. Let me just find the wording and I'll give it right to you. We first asked about the personal ID card.

Mr. HORN. What page are you on?

Dr. WESTIN. This is page 94 of the full report, and you can see that the question first asked about the card, and we got, as I mentioned, the support for the card.

The number question then followed on page 95. "Under national health care reform, each person might be assigned an identification number for health insurance purposes. How concerned would you be to have such a health information number assigned to you?" Very concerned, somewhat concerned, not very concerned or not concerned at all.

You can see that 28 percent of the public would be very concerned if they had such a number and 29 percent somewhat concerned. And traditionally if you combine those two to get the above the line reading, that gives us 57 percent that say they would be concerned.

And then the next question reads exactly, "If there were to be such a number, which would you prefer as an individual health number: Your present Social Security number or a new national health number assigned to each person?" And on that choice, your present Social Security number or new number, you can see that 67 percent of the public would prefer to have their present Social Security number and 30 percent said they would prefer a new national health number assigned to each person.

We could interpret that, read the tea leaves on it, but as you asked, what was the actual wording, that's the way we presented it.

Mr. HORN. One of the things I was thinking of is if there had been a followup question to that question that made the point I'm making, did they understand that these can be linked to other personal documents and does that bother them, sometimes people don't think of that.

Mr. Chairman, if we might, could we just have the relevant tables, tables 9-1 and 9-2, inserted, along with the answer, in the hearing record?

Mr. CONDIT. Without objection.

[The information is contained in appendix 1.]

Mr. HORN. From your research, would the public favor signing a separate authorization form for every disclosure, or how would you work the mechanics of that, based on your study of public opinion and privacy?

Dr. WESTIN. Well, we didn't ask any question about that specifically, so I would have to infer. I would infer that the public, I think, would have two minds. On the one hand, they don't want to be burdened, especially in times of emotional decisionmaking in medical situations, with the kind of requirements of reading notices and signing notices that would be sort of a burden.

On the other hand, I think that most people are concerned about the breadth of current releases and consents and are not comfortable with what some of the present language is, that I release everything to anybody for any purpose forever, and that one of the most important things that legislation can do is to define what is an appropriate consent language, with the appropriate limitations for particular uses.

That's my inference from the structure of views that our survey got, but we didn't ask about that in particular.

Incidentally, these suggestions may be things that we can put into further surveys that we want to do, to test on the number or on the consent form, and those would be very helpful.

Mr. HORN. Now, the groups that you interviewed are obviously fairly knowledgeable about a lot of these practices within some of these institutions.

Dr. WESTIN. The leader sample, yes.

Mr. HORN. And the average public, and I include myself with the average public, are probably not as knowledgeable as to the per-

mutations of this or that form of health care organization, be it a hospital, a doctor's office, an HMO, all the various permutations of that.

What was your impression of the level of knowledge the public might have had about the different types of disclosure that might be asked and how that system works?

Dr. WESTIN. Well, when you ask privacy questions in general, that's always a problem. If you ask about wiretapping, the number of people that actually have had a wiretapping experience is probably going to be very small.

Here, though, I think you have a different situation. The public is composed of people who use health care services, who compile and are aware that there are records about them, that know that they have been asked to disclose health information often to an employer or to an insurance setting or a license setting or a government program.

And so I think that the fact that 27 percent of the public said that they believed that their medical information had been disclosed improperly was really based upon personal experiences and values and attitudes derived from it.

Also, when you have about a quarter of the population that have used mental health services, they're going to be giving you some real live experience as to their concerns about whether sensitive information drawn from psychological and psychiatric services worry them.

So I would attach very high confidence that the kind of questions we asked of the public because they were actually inside their daily life experiences. We asked different questions of the leaders, so we asked them about what kind of information they might want for outcomes research or quality care. We wouldn't expect the public to have real informed judgments about that.

But I would respond that on the questions that we asked, public confidence would be very high, that people know experiences and attitudes they draw on in the answers.

Mr. HORN. One last question, Mr. Chairman, and that is this. You heard the very moving testimony of our colleague, Representative Velázquez this morning. Many of the people you interviewed, as you suggest, also had their personal experiences as a basis for some of their reaction.

From your study of privacy issues, what's the proper type of enforcement, penalty system, if any, that is needed to get conformity to the law or try and be a sufficient deterrent to nonconformity with the law?

In my colleague's bill, the chairman, for whom I have the highest respect, we're talking essentially civil damages, possibly punitive damages, based on the particular court situation. Is that the best route to go? Are there other routes to go? How would you suggest that be handled?

Dr. WESTIN. I think it's very instructive to think about why the episode took place that did in New York. One, I think everybody in the health care system has no experience with anybody every being prosecuted or convicted or being sued for damages successfully for releasing personal medical information. So there's no deterrent in terms of the life experience of people.

So the first thing I think you can do is to put a credible, enforceable mechanism in where some people get indicted and prosecuted, if it's a knowing violation, and some people get sued for damages or lose their jobs because the hospital fires the person that leaked the information about the congresswoman.

So I think it's a combination of creating clear rules with public education going with it, enforcing it, by actually prosecuting people and suing people, and also I thought the answer that it's the hospital's responsibility is a very good answer. They're the first line, and while they can't obviously make sure every time every person obeys their rules, if they can get the people who today breach the rules because they really don't worry about the hospital doing anything about them, you'd make a major step forward. It's that combination, it seems to me, that you really want to achieve.

Mr. HORN. I guess one of my worries is this going to be sort of the tort lawyers' relief act of 1994, when we're trying to get some sense in some of what's going on here? Let's face it. You look at a doctor and you say, "Aha, deep pockets." You look at the modern hospital and you say, "Aha, deep pockets."

Will we just have a lot of this nonsense going on that the institution—doctor, doctor's office, five clerical employees to handle the paperwork of both government and private insurance companies, hospital, thousands of records, hundreds of people might well having access, and in the age of the Xerox machine, you know, if the record was Xeroxed 5 months ago, 5 years ago because someone thought, "Gee, this is the mayor's wife or this is the mayor coming in or a Member of Congress or whatever; maybe I can put that to use." And as the case I cited this morning, if you have a disgruntled employee that's fired, is that not a problem? And you don't know a thing about it, but you've got a bank account. The employee, they can't even find, et cetera. So I'm worried about that.

Mr. BAKER. Mr. Horn, we share your concerns. And in our written testimony we did say that the area of particularly civil damages does appear to perhaps stimulate some of that activity and that perhaps there could be some—and this is one of the areas we'd like to work on—perhaps some method of notice and cure before you get into statutory amounts of \$5,000 and so forth in the damage area, because I think you've expressed a legitimate concern, and we don't want to go down that road. I think you're right.

Mr. HORN. If we wrote into law that the political candidate that used that record would not be able to hold office, even if elected, that might be interesting. It might slow things down. On the other hand, you might have your opponent leaking his own record just to accuse you of doing it. So we run into some of these things.

Well, I thank you all for your testimony.

Mr. CONDIT. Thank you, Mr. Horn. I want to assure you that I'm certainly not trying to create employment for the trial lawyers. Ms. Woolsey.

Ms. WOOLSEY. Very quickly. First, followup to identification numbers. Did you ask the respondents in your survey how often they'd forgotten their ATM number?

Dr. WESTIN. We did not, but obviously behind the idea of "keep my Social Security number" is what you're implying.

Ms. WOOLSEY. Right. I can still remember my Social Security number but I have lost my ATM number every once in a while, so I think we should keep it as simple as possible. Yes?

Mr. BAKER. We were discussing this at some length during the break. There are probably a number of identification systems that are going to be used in different regions and in different health care information environments. And so I'm not sure there's one overall—there may not be one overall identification circumstance.

Ms. WOOLSEY. Maybe we'll try different approaches to it throughout the country until it's clear there's one way to do it that works the best.

Mr. BAKER. Perhaps so.

Dr. WESTIN. That's what I meant, in terms of technologies rolling down, there may be ways of identifying people apart from numbers, such as a thumb print or something which, if the technology becomes widespread and if it's coherent and so forth, that people won't have to remember any numbers. You put your thumb down and you're identified as the right person to use the health system. You carry your thumb with you in most cases.

Ms. WOOLSEY. The grayer my hair gets, the more I'm going to like that. It appears that the public doesn't want us to use their health care records for research, yet we know that research is so important. Do you see that once we get some health reforms in place that the public may accept the idea of using anonymous data for research?

Dr. WESTIN. I think so. I think that what the public is saying is given the way they presently think about the leakiness of the medical record system and about no capacity on their part to control use, it worries them that research might get to their records, because they worry who's the researcher?

If you could have a system of institutional review boards on the research ethics to begin with and then strong legal safeguards against using identified information improperly, my guess is if you put those safeguards to people, and if they believe them, that you would then find a readiness to support research because of all its very valuable social benefits.

Ms. WOOLSEY. So if we start with H.R. 4077 then people may start trusting that their medical information is private.

Dr. WESTIN. Yes, you could retitile this the Trust Restoration Act of 1994, and it might do a great deal for you.

Ms. WOOLSEY. Good. Thank you. Thank you, Mr. Chairman.

Mr. CONDIT. Thank you very much. I want to thank both of you. You've been very helpful and you've been patient with our schedule this morning, and we appreciate that very much.

We have a vote on. The subcommittee has scheduled two additional hearings next week, on Wednesday and Thursday. The witnesses will include representatives of some of the major health care organizations and advocate groups.

Those who cannot be accommodated at the hearing may submit written comments or testimony, and you're welcome to do that. So we'll see some of you next week, and this meeting is adjourned.

[Whereupon at 12:20 p.m., the subcommittee adjourned, to reconvene Wednesday, May 4, 1994.]

THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1994

WEDNESDAY, MAY 4, 1994

HOUSE OF REPRESENTATIVES,
INFORMATION, JUSTICE, TRANSPORTATION,
AND AGRICULTURE SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2247, Rayburn House Office Building, Hon. Gary A. Condit (chairman of the subcommittee) presiding.

Present: Representatives Gary A. Condit, Karen L. Thurman, Bart Stupak, Ileana Ros-Lehtinen, and Stephen Horn.

Also present: Robert Gellman, chief counsel; John Edgell, professional staff member; Aurora Ogg, clerk; and Diane Major, minority professional staff, Committee on Government Operations.

Mr. CONDIT. Good morning.

We have called the meeting to order. This is the second legislative hearing on H.R. 4077, Fair Health Information Practices Act of 1994.

At our last hearing we received a positive assessment of the legislation from the administration, and we heard the results of the very timely public opinion poll on medical privacy issues.

Today we continue with the witnesses from the major medical institutions that will be directly affected by the legislation; we will hear from doctors, hospitals, insurers, and medical record professionals.

A second panel will bring in the views of a major employer, a private foundation with considerable amount of experience in maintaining and disclosing sensitive patient information, and a law professor who will be able to comment on how confidentiality issues are addressed elsewhere in the world.

We will be joined a little bit later by the other members of the committee, but in consideration of your time and our time up here, we're going to go ahead and begin.

So this morning we have the first panel, Ms. Frawley, Mr. Gimpel, Mr. Entin, and Dr. Lewers.

Some of you appeared before this committee a few months ago and we're delighted and honored that you're back again, and we do appreciate greatly your participation in this issue. It has been very helpful to the committee.

So I am going to allow you to make your comments, and then if the other members come, we will let them make their opening statements at the end of this panel.

We have a policy of this committee, and some of you are already aware of this policy, those of you who are not, don't be alarmed. We swear all witnesses in. So will you please rise and raise your right hand.

[Witnesses sworn.]

Mr. CONDIT. Dr. Lewers.

STATEMENT OF DONALD LEWERS, M.D., MEMBER, BOARD OF TRUSTEES, AMERICAN MEDICAL ASSOCIATION

Dr. LEWERS. Thank you, Mr. Chairman. It's a pleasure to be back with you.

I am Donald T. Lewers. I am an internist and kidney specialist in Easton, MD, and a member of the board of trustees of the American Medical Association.

Physicians have an essential role in preserving patient privacy. That is why we applaud your commitment to the sensitive subject, Mr. Chairman, and express our gratitude for involving the medical profession in developing the Fair Health Information Practice Act of 1994.

Confidentiality is fundamental ethical tenant of the physician/patient relationship. People must have the confidence that their conversations with their doctors will not be broadcast or in any way compromised.

Without such free communication, physicians will not be as readily able to diagnose and manage many illnesses. Efforts to protect this information often set out in the medical records must be escalated.

This is why, Mr. Chairman, the AMA applauds your sponsorship of H.R. 4077. This legislation would establish a reasonable Federal role through the development of a code of fair information practices that will help to ensure the privacy and security of patient health care information.

The AMA concurs with the need for precise accounting procedures regarding disclosure of protected health information to ensure that unbridled dissemination of individually identifiable health care data does not occur.

We further commend you in creating appropriate guidelines for disclosure of protected health information to law enforcement authorities. We agree that mandatory blanket transmission of comprehensive health care data in this area without permitting the health information trustee to utilize boundaries crafted in section 129(a) would be improper.

The provision in H.R. 4077 applying to information disclosure are effectively bolstered by directing health information trustees to incorporate reasonable safeguards to ensure the integrity and confidentiality of protected health information. The proposed security measures are important to further insulate private health care data from unauthorized access.

With the increasing computerization of patient records and changes in medical record creation and use, we must make certain that legal and ethical precepts applicable to paper records are not lost. Patient records, regardless of form, must always remain confidential and free from unauthorized access. We feel that it is a given that even more complex security measures will be required

to protect patient privacy with the move to computerized-patient records.

We appreciate your interest in addressing the issues inherent in this critical patient care matter. However, we are concerned that the rush to simplification and standardization in the way health insurance claims are processed and patient records are handled, may compromise our role as the advocate our patients' interest.

Care must be taken to avoid creating added levels of bureaucracy to administer these programs. We can ill afford to impose undue economic burdens upon physicians or health care providers to implement electronic data systems. Similarly, recognized and successful reporting mechanisms should not be recreated.

Finally, legal restrictions that provide maximum protection for patient—for the patient, must be clearly articulated. At a minimum, we must have the following protective factors:

Restrictions on access to information must be clearly established; information released for one purpose must not be used for another purpose; where disclosures of health care information occur, principles of informed patient consent still must apply; when a health care record is shared, any risk that a patient could be identified must be minimized; for research purposes, data must be supplied in aggregate form with removal of individual identifiers.

In conclusion, we strongly believe that the protection from any unauthorized disclosure must be vigorously pursued. For example, the sanctity of the information that may be assessable through the health security card must be protected. The health security card must not become an avenue for access to personal, private and privileged information about an individual.

We are convinced that with appropriate safeguards computerized-patient records can provide a valuable service by assisting physicians and the health care community in reaching our goal of providing the highest quality medical and health care. However, we want to underscore that confidentiality protection will be critical in the new environment that will be created under health system reform.

The AMA appreciates the opportunity to appear before the subcommittee and we will be pleased to respond to questions.

Mr. CONDIT. Thank you, Dr. Lewers. We appreciate your being here.

[The prepared statement of Dr. Lewers follows:]

American Medical Association

Physicians dedicated to the health of America



515 North State Street
Chicago, Illinois 60610

Statement

to the

Subcommittee on Information, Justice, Transportation,
and Agriculture
Committee on Government Operations

U. S. House of Representatives

**RE: H.R. 4077 -- FAIR HEALTH
INFORMATION PRACTICES ACT OF 1994**

Presented by: Donald T. Lewers, MD

May 4, 1994

Division of Federal Legislation
312 464-4775

STATEMENT

of the

AMERICAN MEDICAL ASSOCIATION

to the

Subcommittee on Information, Justice, Transportation, and Agriculture
Government Operations Committee
United States House of Representatives

Presented by

Donald T. Lewers, MD

RE: H.R. 4077 -- Fair Health Information Practices Act of 1994

May 4, 1994

Mr. Chairman and Members of the Subcommittee.

My name is Donald T. Lewers, MD. I am an internist and kidney specialist in Easton, Maryland and a member of the Board of Trustees of the American Medical Association (AMA). Accompanying me is Hilary Lewis, JD, of the AMA's Division of Federal Legislation.

On behalf of the AMA, I am pleased to have this opportunity to express our views regarding the critical issues of privacy and confidentiality, particularly in the new environment that will be created under health system reform. We applaud your commitment to this sensitive subject, Mr. Chairman, and express our gratitude for seeking the involvement and participation of the medical profession in every phase of your initiative -- from your initial examination of the topic through the development and introduction of H.R. 4077, the "Fair Health Information Practices Act of 1994."

The AMA has long been concerned with the myriad of issues involving confidential patient information and the quintessential role of the physician in preserving patient privacy as a major component in rendering quality medical care. Confidentiality of the health care information contained

in the patient medical record, whether that record is generated through care delivered in the public or the private sector, remains a cornerstone of the physician/patient relationship. Underlying any discussion of confidentiality is the need for patients to be willing to tell their physicians highly personal, possibly embarrassing, and deeply private information. Without such free communication, physicians will not be able to properly diagnose many illnesses. People must have confidence that they can speak to their doctors without that information being made available. As the ability to computerize medical records expands and is used, the potential for confidentiality breaches heighten, and efforts to protect and maintain confidentiality of all medical records similarly must be escalated.

The AMA has long been active in pursuing matters regarding patient privacy and looks forward to participating with Congress and the Administration as health system reform continues to evolve. Opinions articulated by the AMA Council on Ethical and Judicial Affairs (CEJA), development of AMA model state legislation on the confidentiality of health care information, ongoing activity regarding the AMA Physician Masterfile, and reports of the AMA Council on Scientific Affairs have highlighted confidentiality issues from a variety of perspectives. We were also pleased to participate in the efforts of the Workgroup on Electronic Data Interchange (WEDI) convened by the Department of Health and Human Services (HHS) in 1992 to explore the use of electronic claims processing as a mechanism to increase efficiency, reduce costs, and improve patient service. The AMA was actively engaged in the Department of Health and Human Services Workgroups on Computerized Patient Information and External Performance Monitoring as well. The AMA was also a founding member of the Computer-based Patient Record Institute and serves on its governing board.

ETHICAL ISSUES

Confidentiality is a fundamental tenet of the physician/patient relationship, underlying the ethical context of all communication that takes place during the course of medical care and treatment

The AMA Principles of Medical Ethics declare.

A physician shall respect the rights of patients, of colleagues, and of other health professionals, and shall safeguard patient confidences within the constraints of the law

As stated in Opinion 5.05 of the AMA Council on Ethical and Judicial Affairs:

The information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree. The patient should feel free to make a full disclosure of information to the physician in order that the physician may most effectively provide needed services. The patient should be able to make this disclosure with the knowledge that the physician will respect the confidential nature of the communication. The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law.

Physicians recognize that a patient's history, diagnosis, treatment, and prognosis may be discussed with a patient's attorney with the consent of the patient or the patient's lawful representative. Additionally, a physician may disclose history, diagnosis, and prognosis of a patient to an insurance company representative, but only if the patient or a lawful representative of the patient has consented to the disclosure (Opinion 5.08). Ethical opinions further clarify that a physician's responsibilities to patients are not limited to the actual practice of medicine, and include the performance of some services ancillary to medical practice, such as certification that the patient was under the physician's care, and comments on the diagnosis and care in a particular case.

A panoply of other ethical issues related to patient record confidentiality have also been addressed in our ethical opinions: (1) availability of the physician record to other physicians; (2) disposal and transfer of patient records upon a physician's retirement or sale of a medical practice; (3) confidential information obtained by a physician in an employment setting; (4) the physician's responsibility to testify in court or before a worker's compensation board in a personal injury or related case regarding confidential patient information, and (5) the application of confidentiality to computerized medical records.

One abiding ethical principle remains clear:

Notes made in treating a patient are primarily for the physicians's own use and constitute his

or her personal property. However, on request of the patient, a physician should provide a copy or a summary of the record to the patient or to another physician, an attorney, or other person designated by the patient. (Opinion 7.02)

The opinion further declares

The record is a confidential document involving the physician-patient relationship and should not be communicated to a third party without the patient's prior written consent, unless required by law or to protect the welfare of the individual

The ethical principles outlined above have been embodied in a number of state statutes, as well as in AMA model state legislation on the confidentiality of health care information (ATTACHMENT A). State laws have also incorporated provisions authorizing patient access to the medical record, with many outlining specific limitations regarding access to psychiatric records, records of minor patients, and communicable disease information. Due to the lack of uniformity that exists under the framework of state laws, the AMA advises physicians to "become familiar with the applicable laws, rules, or regulations on patient access to medical records" (Opinion 7.02).

COMPUTER-BASED PATIENT RECORDS

With computer technology applied to the medical record arena, and full computerization of patient records becoming a reality, medical record creation and use in health care delivery will inevitably change. Certain legal and ethical precepts applicable to the paper medical record, however, will remain relevant to records generated and modified on computer, signed or authenticated via computer, stored on computer media, and retrieved by computer. Regardless of the form they may take, patient records must always remain: (1) confidential; (2) accurate and comprehensible; (3) secure; and (4) free from unauthorized access. The AMA appreciates the interest of the Subcommittee in addressing this critical issue.

The 1991 Institute of Medicine (IOM) Report, The Computer-Based Patient Record: An

Essential Technology for Health Care¹, applauds "the detailed and ethically sensitive" guidelines for computerized patient databases outlined by the AMA in CEJA Opinion 5.07 (ATTACHMENT B)². These guidelines for maintaining confidentiality of health information in the electronic data environment specify that: (1) the physician and the patient must consent to the release of patient-identifiable clinical and administrative data to any entity outside the medical care environment, (2) release of confidential health information should be confined to the specific purpose for disclosure, and (3) recipients of information should be advised that any further disclosure is improper. As patient records become fully computerized, it is even more imperative that safeguards are taken to preserve confidentiality.

1. Legal and Ethical Confidentiality Requirements

The legal sources of confidentiality rules may be traced primarily to state medical practice acts which subject a physician to professional discipline for failing to preserve the confidentiality of patient records.³ A physician member of a hospital medical staff who creates or obtains access to patient records is also subject to confidentiality requirements largely found in state hospital licensing statutes⁴ and regulations,⁵ and accreditation standards of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO).⁶ State medical records acts establish confidentiality guidelines in

¹ The Computer-Based Patient Record: An Essential Technology for Health Care, Institute of Medicine, 1991.

² Ibid p. 162.

³ Ill. Rev. Stat. ch. III, §4400-22.30 (1987)

⁴ Ann. Code of Md. §4-301 (1990)

⁵ Ill. Hosp. Licensing Requirements §12-1 2(b) (1979); Utah Hosp. Rates and Regulations, §7.402 et seq. (1984).

⁶ JCAHO MR 3.1 MR 3.2 (1993).

varying degrees for hospital records and physician office medical records as well.⁷ Medicare regulations,⁸ the Federal Privacy Act,⁹ and the federal alcohol and drug abuse statute¹⁰ impose standards of confidentiality that also apply to medical records, such as the special confidentiality rules that apply to records of patients who seek drug or alcohol treatment at federally funded facilities. Under the common law, numerous court decisions have held that the physician/patient relationship is characterized by its fiduciary nature, thus obligating the physician to retain in confidence personal information regarding the patient, including data contained in the patient record. Any unauthorized disclosure of such information may, therefore, subject the physician to liability for breach of trust or invasion of privacy.

Exceptions to statutory confidentiality requirements generally permit disclosure under controlled circumstances, with the release of medical information restricted to the purpose of the disclosure. As stated earlier, medical records may be disclosed with the consent of the patient or the patient's authorized representative. Disclosure may also be required pursuant to: (1) government reimbursement programs; (2) mandates of state licensing agencies; (3) the federal Peer Review Organization (PRO) program; and (4) public health reporting laws relating to child abuse, AIDS, controlled substances, occupational diseases, cancer, birth defects, and gunshot wounds.

2. The Legal Necessity of Computer Security

As the members of this Subcommittee know, notwithstanding the many federal and state statutory and regulatory requirements, computerized patient records (CPRs) will require even more

⁷ Ill. Rev. Stat. Ch 110 §8-2001-2003 (1980).

⁸ 42 CFR §482.24 (b) (3).

⁹ 5 USC §552a (1988).

¹⁰ 42 USC §§290dd-3, 290ee-3 (1988).

complex security measures both to protect patient privacy and to avoid adverse legal consequences

If a CPR system lacks reasonable security in design or operation, the records stored on the system may not be deemed sufficiently reliable to be introduced as evidence in court. Introduction of computer viruses and other security breaches may compromise the accuracy of patient records as well. Computer sabotage can lead to slowdown or collapse of a system such that users will be denied access to health records. The resulting inaccessibility to necessary medical data may ultimately bring harm to the patient. With computer technology and concomitant security devices continually evolving, however, a legal standard of reasonableness should be applied to any computer security measures undertaken.

3. Keeping Computerized Records Confidential and Secure

Computers have the capacity to store, copy, and transmit massive amounts of patient health information. At the same time, electronic data collection has the potential to restrict access to sensitive information and limit its use to authorized individuals. Even a single breach in the security of a computerized patient record (CPR) system, however, may result in the disclosure of a vast number of medical records. CPR systems in hospitals and physicians' offices, moreover, demand that various individuals be involved in data entry. As each hospital department or physician office in which portions of a record are generated becomes computerized, and with care being provided in diverse settings, access to the record from multiple locations is increased. While such remote access capability optimally should enhance patient care, security measures must be employed that balance the need for confidentiality with the necessity for quick and easy access by physicians and other patient care professionals.

The following security measures should be taken to enhance the security of any CPR system:

- (1) A CPR system should only permit authorized users to access medical records through the use of frequently changed passwords, access codes, and/or key cards;
- (2) Hospitals and physicians' offices should adopt and strictly enforce policies against disclosing

or sharing passwords, access codes, and key cards.

- (3) Upon termination of employment, passwords and access codes should be immediately deactivated;
- (4) The access of each user should be limited to the portions of the patient record relating only to the user's responsibility in the hospital or medical practice;
- (5) A CPR system should be programmed so that records may not be retrieved beyond one's clearance, with user access to records monitored on an ongoing basis as a disincentive to unauthorized viewing of records;
- (6) Use of software should be restricted to permit copying of only one record at a time;
- (7) Networking and electronic data sharing programs with outside computers from different institutional settings should institute adequate privacy safeguards prior to transmission to reduce the risk of computer sabotage and to ensure that such information is appropriately exchanged for delivery of optimal patient care; and
- (8) Anti-virus software to detect and block computer viruses and other forms of sabotage should be utilized.

4 Confidentiality and the Physician/Patient Relationship

With confidentiality as a cornerstone underlying the physician/patient relationship, it should be no surprise that the AMA has assumed a leadership role in protecting the confidentiality, integrity, and security of patient-specific information. Privacy and confidentiality are critical to every aspect of the physician/patient relationship.

We believe that electronic data management activities can serve an important function in yielding more time for our paramount concern -- the provision of quality health care to our patients. As health system reform evolves and more patients are treated through managed care entities and large group practices, the role of the physician remains constant -- as the advocate of patient interests. In this capacity, the physician may not necessarily record every aspect of the patient encounter, employing self-imposed restraints consistent with professionalism. The physician's commitment to use data in the proper fashion serves to further protect patient confidentiality.

LEGISLATIVE PROPOSALS

Simplification and standardization in the way health insurance claims are processed and patient records are handled can bring about significant cost-savings. However, micromanagement of the information system at the federal level will diminish any savings that could be realized, and the AMA opposes such a broad federal role. We believe the costs of developing any type of information management system must be recognized. We must be vigilant, moreover, to avoid creating additional levels of bureaucracy to administer these programs or imposing undue economic burdens upon physicians or health care providers to implement electronic data systems, especially where they may recreate recognized and successful reporting mechanisms. For example, the means commonly accepted for reporting physician services, *Physicians' Current Procedural Terminology (CPT)*, is already recognized by the Department of Health and Human Services for use in the Medicare and Medicaid programs, and any other coding system formulation, would be redundant. Just as the AMA works with the Health Care Financing Administration and others to maintain CPT, we are committed to efforts to ensure that computerized patient record systems, as well as related legislation and regulations, include adequate technical and legal safeguards to protect the quality, confidentiality, integrity, and security of patient data.

1. Workgroup on Electronic Data Interchange

The Workgroup on Electronic Data Interchange (WEDI) issued a number of recommendations to assure that electronic data interchange (EDI) for health care claims processing and payment does not compromise data confidentiality or privacy rights of patients, their physicians, or health care providers. We believe that the proposals of the WEDI Confidentiality Workgroup merit careful consideration in formulating any approach to address broader questions of privacy of private sector health records. Given the current patchwork of state statutes and regulations on medical record confidentiality, the Workgroup recommended the development of federal preemptive legislation that

would.

- (1) establish uniform requirements for preservation of confidentiality and privacy rights in electronic health care claims processing and payment;
- (2) apply to collection, storage, handling, and transmission of identifiable health care data, including initial and subsequent disclosures in electronic transactions by all public and private third-party payers, health care providers and all other entities;
- (3) not apply to state public health reporting laws;
- (4) delineate protocols for secure electronic storage and transmission of health care data;
- (5) specify fair information practices to ensure a proper balance between required disclosure and use of data;
- (6) require publication of the existence of health care data banks;
- (7) establish appropriate protections for highly sensitive data, regarding, for example, mental health, substance abuse and communicable diseases;
- (8) encourage use of alternative dispute resolution mechanisms where appropriate;
- (9) establish that compliance with the requirements of this legislation constitute a defense to actions for improper disclosure;
- (10) establish penalties for violations of this legislation, including civil damages, equitable remedies and attorneys' fees, where appropriate; and
- (11) provide for enforcement by government officials and private aggrieved parties.

One of the key areas in which government can help ensure the health care system works competitively and efficiently is by working in partnership with all those involved in health care -- physicians, hospitals, other professionals and providers, insurers, and consumers. The WEDI effort serves as a model for this activity in bringing together representatives from throughout the health care industry to cooperate in mobilizing the industry's use of technology to streamline the administration of health care. This process is indicative of the kind of cooperation and partnership that must occur if meaningful change in the way our health care system is administered can be effected.

2. H.R. 4077: the "Health Information Practices Act of 1994"

Mr. Chairman, the AMA applauds your sponsorship of H.R. 4077, the "Health Information

Practices Act of 1994." This legislation would establish a reasonable federal role through the development of a code of fair information practices for health information. The code would constructively define the rights of individual subjects of such information created or maintained as part of the treatment and payment process. The Act also would delineate the rights and responsibilities of those who create or maintain individually identifiable health information that originates or is used in this process, as well as construct effective mechanisms to enforce these rights

a. Code of Fair Information Practices/Authorized Disclosure

The code of fair information practices contained in H.R. 4077 will help to ensure the privacy and security of patient health care information. Assigning responsibility to the health information trustee who creates or receives protected health information to prepare a written notice of information practices describing: (1) the right of the individual to inspect and copy information; (2) the right of the individual to seek amendments to such information; and (3) the procedures for authorizing disclosures of protected information and for the revocation of such disclosures, would buoy consumers with greater assurance that their private information, irrespective of the form in which it is recorded, will be accessible for their personal use, yet shielded from unauthorized disclosure.

The AMA also concurs with the need for precise accounting procedures regarding disclosure of protected health information as set forth in the bill. Requiring the maintenance of records regarding the date and purpose of any disclosure, the name and address of the person, or location to which the disclosure was made, and the information disclosed, will help to ensure that unbridled dissemination of individually identifiable health care data does not ensue by conserving the identity of the recipients.

We further commend the bill for imposing a mandate upon the health information trustee to use protected information only for purposes for which it was collected. The parameters limiting disclosure to the minimum amount of information necessary to achieve the objective for which it is

used or disclosed, serve to appropriately foreclose the potential for the blanket release of unabridged health care information. An authorization for disclosure by the subject of such information on a discrete form separate from those documents governing health care consent or payment, and expressly naming both the trustee and the recipient of the information, will confer maximum patient control over the health record contents. Requiring that the prospective recipient of such information submit a statement outlining its intended uses and disclosures creates even stronger conditions attached to its use.

The "Fair Health Information Practices Act of 1994" also circumscribes guidelines for disclosure by the health information trustee to next of kin, to public health officials for disease reporting and surveillance purposes, in emergency circumstances, for health research activities, and for directory information. In Section 129 of the bill, appropriate guidelines for disclosure of protected health information to law enforcement authorities are also outlined. Mandatory blanket transmission of comprehensive health care data in this area, absent the exercise of discretionary authority by the health information trustee utilizing the boundaries crafted in Section 129(a), would be improper.

b. Safeguards for Security

The provisions in H.R. 4077 applying to information disclosure are effectively bolstered by directing health information trustees to incorporate reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of protected health information and guard against threats or hazards of improper disclosure. Some of these security measures would include regular training in the requirements that govern such information for those employed by or affiliated with the trustee. The maintenance of audit trails, as well as the posting of signs and warnings accompanied by advice regarding the necessity to secure protected information, are prescribed to further insulate private health care data from unauthorized access. The AMA

applauds the bill for addressing matters relating to unauthorized employee access to patient information.

c. Development of Regulations

The "Health Information Practices Act of 1994" designates the Secretary of Health and Human Services (HHS) to develop and disseminate a model notice of information practices for use by health information trustees. The HHS Secretary would also be required to issue guidelines for disclosure of protected health information and model statements of intended uses and disclosures for those who wish to receive health information from a health information trustee. All of these guidelines are to be developed by July 1, 1996, after notice and opportunity for public comment.

The AMA strongly recommends that any guidelines or model statements that are drafted to ensure the privacy of health care information be developed through a negotiated rulemaking process pursuant to the dictates of the Negotiated Rulemaking Act of 1990, 5 U.S.C. §561 et. seq., rather than through the traditional procedures established in the Administrative Procedure Act, 5 U.S.C. §551 et. seq. The 1990 Act permits federal agencies to utilize negotiated rulemaking as an alternative to public notice and comment rulemaking prescribed by the federal Administrative Procedure Act. Under negotiated rulemaking, the affected parties would meet with the Department of Health and Human Services and formulate an initial draft regulation. That regulation would then be offered for public notice and comment.

Negotiated rulemaking thus offers an opportunity to expedite the regulatory process by crystallizing the views and expertise of those who are most knowledgeable in a given area, prior to the issuance of a notice of proposed rulemaking. In the sensitive area of privacy and confidentiality, a collaborative endeavor early in the rulemaking process would be especially constructive in articulating rules that represent an amalgam of current thinking by experts in this field. The effective date for implementation of H.R. 4077 has been set at January 1, 1997, a full six months after the

regulations must be drafted. This timing is suitable inasmuch as fair information standards and confidentiality guidelines would be developed prior to the effective date of the measure. Negotiated rulemaking would enhance the ability to meet these deadlines by integrating the views of those most involved in preserving the sanctity of health care information.

d. Privacy and Security Standards

The AMA continues its longstanding support for the creation of privacy and security standards relative to health care information, and stresses the importance of developing fair and comprehensible authorization and consent forms for the disclosure and redisclosure of information to authorized persons, for authorized purposes, at authorized times. The definition of "protected health information" contained in H.R. 4077 encompasses any information, whether oral or recorded, in any form or medium that:

- (A) is created or received by a health care provider or a public health trustee in a State; and
- (B) relates to the past, present, or future physical or mental health of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual and --
 - (i) identifies the individual; or
 - (ii) with respect to which there is a reasonable basis to believe that the information can be used readily to identify the individual.

In view of the increasing usage of data collection and transmission in electronic form, we believe that any legislative proposal (as reflected in the bill now under discussion) designed to develop standards to ensure uniform, confidential treatment of individually identifiable health care information, must address all methods in which health care information is presently recorded. In fact, expanded standards specifically relating to EDI indeed may be optimal. The safeguards for security outlined in the "Fair Information Practices Act of 1994" recognize the need to adequately buttress health care data from potential security breaches, yet balance the concomitant need for "reasonable and appropriate" security mechanisms. Due to the burgeoning nature of electronic data information and the dynamic technological innovations that are being advanced to augment the protections that

many EDI systems currently employ, such standards should be subjected to ongoing review and appropriate modification on a regular basis. In this regard, the creation of an advisory panel, comprising representatives of the public and private sector, could act as a valuable resource for updating the standards and requirements for emerging technology. Any such entity should, of course, include membership of the health care professional and provider communities. The AMA possesses the expertise, the track record, and the resources to provide physician input to a joint public/private sector effort of this kind.

e. Patient Education

We also believe that any approach formulated must include a patient education program to provide information to all participants in the health care system regarding the privacy of health record information. The written notice of information practices that health information trustees would be required to prepare under H.R. 4077 represents a constructive start to a patient education model. However, more comprehensive programs must be devised to ensure that the public clearly understands the complexities associated with the protection of health care information. The AMA would be pleased to assume an active role in such an informational endeavor.

f. Enforcement Provisions

The enforcement provisions in the bill would permit the recovery of actual damages for a knowing violation, with punitive damages and attorney fees also available to the prevailing party. A health information trustee who has been determined by the Secretary of HHS to fail to substantially comply with the provisions of the measure would be subject to a civil monetary penalty of up to \$10,000 for each violation. Alternative dispute resolution methods will be developed to resolve claims for civil monetary penalties in a fair, timely, and affordable manner. Finally, criminal sanctions are included in H.R. 4077 for those who secure monetary gains from obtaining protected health information under false pretenses, for knowing and unlawful obtaining of protected health

information, for knowing and unlawful use or disclosure of protected health information, and for securing monetary gain from knowing and unlawful sale, transfer, or use of protected health information

The AMA believes that the penalty provisions for statutory violations are appropriate. However, we strongly urge the creation of an oversight mechanism, to assist the Secretary in making determinations regarding substantial compliance and to provide periodic reports to this Committee and the Congress evaluating the status and utility of the fair practices incorporated in the measure.

g. Federal Preemption

The AMA urges modification of the federal preemption provision contained in Section 304 of HR 4077. The bill declares that state law cannot be established, continue to be effective, or be enforced:

to the extent such law is inconsistent with a provision of this Act, but nothing in this Act shall be construed to indicate an intent on the part of Congress to occupy the field in which its provisions operate to the exclusion of the laws of any State on the same subject matter

Many of the problems relating to confidentiality and privacy of health care information can be traced to the patchwork of inconsistent state laws that have been enacted on this subject. Both in the current environment and under health system reform, interstate electronic data transfer and transmission will intensify. Without the enactment of strong federal preemptive legislation in this area, the potential for breaches of security and privacy will be exacerbated. The AMA, therefore, recommends that state statutes that are as strict as, or contain even more stringent levels of confidentiality protection than the standards incorporated in this measure, should not be preempted. Where such levels of protection do not exist, the "Fair Information Practices Act of 1994" should preempt state law.

3. EDI Implementation: The AMA View

The AMA believes that a legislative solution must similarly address the critical issues of implementing an EDI system. Although change is imminent, it is not possible overnight. A fixed

time limit should not be set for private sector adoption of EDI. We also urge the creation of tax incentives and other policies to encourage the implementation of EDI. If the goal is to control costs and lessen administrative burdens, implementation should not force physicians or providers to incur sudden costs or utilize new and untried reporting mechanisms which will only result in increased health care spending.

The AMA does not support mandatory implementation of EDI. Attached to this statement is a recent study on the extent of electronic billing among physicians. (ATTACHMENT C) Without a mandate, without incentives other than cost-savings and simplicity, and without a uniform format of software packages, the percentage of physicians whose practices submit claims and have electronic billing capabilities has increased from 42.2 percent to 49 percent in only one year, from 1991 to 1992. We have no doubt that trend will continue. The marketplace and competition have created this movement. Any government involvement should help to encourage this transition, not preempt it.

4. Restrictions on Access to Information

Appropriate restrictions on access to information must be formulated in any system that is created so that patient confidentiality is not compromised. As stated earlier, H.R. 4077 addresses a variety of issues involving limitations on disclosure of health care data specifically addressing both the recipient of the recorded material and the precise circumstances surrounding the disclosure. These boundaries will protect the privacy of patients and ensure the confidentiality of information in the data interchange system. It is imperative that information released for one purpose not be used for another purpose. With respect to patient preauthorization for the release of health care information, we believe that principles of informed consent must apply. Legal restrictions that provide maximum protection for the patient must be clearly articulated. In order that reimbursement occur for a valid medical event, only necessary payor information should be conveyed. The volume of information disclosed for the purpose of third-party payment should be limited to the patient's name, other

identifying information, procedure, and diagnosis information. When a health care record is shared, any risk that a patient could be identified from the data should be minimized. For research purposes, data should be supplied in aggregate form with removal of individual patient identifiers. Protections from further unauthorized disclosures must be incorporated and vigorously enforced.

The issuance of a national health security card to every American to guarantee access to needed health services contains merit in terms of facilitating passage through the health care delivery system and receipt of information about health coverage through an integrated national network. We concur with the need to restrict the scope of information contained on this card. We urge Congress and the Administration to ensure that safeguards be established so that a health security card does not become a vehicle for accessing other types of information about an individual.

AMA PHYSICIAN MASTERFILE

Finally, as this Subcommittee addresses the issue of patient record privacy, it may be useful to examine matters relative to physician information as well. Security of information pertaining to physicians is carefully maintained through the American Medical Association Physician Masterfile. This is the most comprehensive source of physician information available in the United States. It has been in existence since 1905 and contains demographic, educational, and current practice information on all of the 665,000 physicians eligible to practice medicine in this country.

At the heart of each record is the Medical Education Number (ME#). The ME# is a unique identifier assigned to every U.S. physician upon entry into medical school and to every foreign trained physician who enters a residency training program in the U.S. The AMA's constructive relationships with U.S. medical schools, graduate medical education programs, and the Educational Commission for Foreign Medical Graduates facilitate and ensure the accuracy and comprehensiveness of this information. Our data are based on primary source information, with contributions from thousands of data providers. These resources ensure that any errors that may occur are corrected

immediately.

The ME# also compares favorably with the Medicare Unique Physician Identifier Number (UPIN) in the following ways:

- An ME# has been assigned to all 665,000 U.S. physicians. A UPIN has been assigned to only 515,000 physicians.
- The Masterfile contains current practice, historical, and demographic information on each physician verified with primary sources. The UPIN file contains only the name, city, state, and zip code of each physician.
- The Masterfile has been in existence since 1905. The UPIN file is less than two years old and remains untested.

The AMA believes that our Physician Masterfile may serve as a model for any computerized record system, both in its capacity to store comprehensive information and in its ability to maintain updated information and to observe appropriate security restrictions regarding this information. Recent proposals for the federal government to develop unique identifiers for each health care professional and provider, moreover, would be redundant inasmuch as physicians already are identified by the ME#, and many hold UPIN identifiers. Accepted identifiers need not be duplicated.

CONCLUSION

Computerization of patient records raises numerous security and medical record confidentiality issues. The "Fair Health Information Act of 1994" reflects a realistic and cogent approach to the critical issue of maintaining patient privacy in the context of patient medical records. The AMA believes that any recommendations that are ultimately formulated should combine both technological and practical patient protection concerns. It is essential that the high costs associated with security systems and the necessity that records be easily accessible by health professionals be considered. The need to protect patient confidentiality, record security, and integrity must be balanced with the practical constraints of achieving perfect security or confidentiality. To properly strike this balance, the AMA recommends that physicians and other health care providers should be expected to use

reasonable mechanisms (there is no failsafe approach) for computer-based patient records. With appropriate safeguards, computerized patient records can provide a valuable service by assisting the health care community in reaching its goal of rendering the highest quality medical care. The development of fair information practices for health care information, as reflected in H.R. 4077, would represent a sound and constructive approach to ensuring uniform, confidential treatment of individually identifiable health care information, especially in the pervasive EDI environment that promises to dominate the future of medical record collection.

Physicians have already taken the first steps into a new frontier in the way medicine is practiced, through efforts that mirror the profession's long history of voluntary efforts to improve the quality of medical care. Government should not unnecessarily try to duplicate or supplant these efforts. This should be achieved in partnership with physicians and others dedicated to effecting health system reform, helping to ensure that these efforts are successful.

The AMA appreciates the opportunity to appear before this Subcommittee. At this time, we will be pleased to respond to questions.

to the

Subcommittee on Information, Justice, Transportation,
and Agriculture
Committee on Government Operations

U. S. House of Representatives

**RE: H.R. 4077 -- FAIR HEALTH
INFORMATION PRACTICES ACT OF 1994**

Presented by: Donald T. Lewers, MD

May 4, 1994

IN THE GENERAL ASSEMBLY
STATE OF _____

A Bill

To Provide For Confidentiality
of Health Care Information

1 Be it enacted by the People of the State of _____, represented in the General
2 Assembly:

3 Section 1. This act may be cited as the "Confidentiality of Health Care Informa-
4 tion Act".

5 Section 2. The purpose of this Act is to establish safeguards for maintaining the
6 integrity of confidential health care information. The necessity of keeping patient health
7 care information confidential and free from unauthorized access exists regardless of
8 whether the records are kept on paper, preserved on microfilm or are stored in computer-
9 retrievable form.

10 Section 3. For purposes of this Act —

11 (a) the term "health care provider" means any person, corporation, facility or
12 institution licensed by this state to provide or otherwise lawfully providing health care
13 services, including but not limited to a physician, hospital or other health care facility,
14 dentist, nurse, optometrist, podiatrist, physician therapist or psychologist, and an officer,
15 employee or agent of such provider acting in the course and scope of his employment or
16 agency related to or supportive of health care services;

17 (b) the term "health care services" means acts of diagnosis, treatment, medical
18 evaluation or advise or such other acts as may be permissible under the health care
19 licensing statutes of this state;

1 (c) the term "confidential health care information" means information
2 relating to a person's health care history, diagnosis, condition, treatment or
3 evaluation, regardless of whether such information is in the form of paper,
4 preserved on microfilm or are stored in computer-retrievable form;

5 (d) the term "medical peer review committee, means a committee of a
6 state or local professional medical society or of a medical staff of a licensed
7 hospital, nursing home or other health care facility provided the medical staff
8 operates pursuant to written bylaws that have been approved by the govern-
9 ing board of the hospital, nursing home or other health care facility, or other
10 organization of physicians formed pursuant to state or federal law and autho-
11 rized to evaluate medical and health care services; and

12 (e) the term "third party" means a person or entity other than the
13 person to whom the confidential health care information relates and other
14 than a health care provider.

15 **Section 4.** (a) Except as provided in subsection (b) or as otherwise
16 specifically provided by law, a person's confidential health care information
17 shall not be released or transferred without the written consent, on such a
18 consent form meeting the requirements of section 4 (d) of this Act, of such
19 individual or his authorized representative. A copy of any notice used
20 pursuant to section 4 (d), and of any signed consent shall be provided to the
21 person signing a consent form.

22 (b) No consent for release or transfer of confidential health care infor-
23 mation is required in the following situations: (1) to a physician, dentist, or
24 other medical personnel for diagnosis or treatment of such individual in a
25 medical or dental emergency, or (2) to medical peer review committees, or
26 (3) to a State Insurance Department or other state agency for the purpose of
27 reviewing an insurance claim or complaint made to such Department or other
28 agency by an insured or his authorized representative or by a beneficiary or
29 his authorized representative of a deceased insured, or (4) to qualified per-
30 sonnel for the purpose of conducting scientific research, management audits,
31 financial audits, program evaluations, or similar studies, but such personnel

1 shall not identify, directly or indirectly, any individual patient in any report of such
2 research, audit, or evaluation, or otherwise disclose patient identities in any manner
3 (the term "qualified personnel" means persons whose training and experience are
4 appropriate to the nature and level of the work in whose training and experience
5 are and who, when working as part of an organization, are performing such work
6 with published and adequate administration safeguards against unauthorized disclo-
7 sures), (5) by a health care provider, as reasonably necessary in the provision of
8 health care services to a person, or in the administration of the office or practice or
9 operation of a health care provider (as used herein, "administration, reimburse-
10 ment, liability risk management or appraisal, and defense or prosecution of legal
11 actions), (6) by an employer as reasonably necessary in the administration of a
12 group insurance or workmen's compensation plan, (7) upon the filing of a claim
13 for insurance benefits, between third party insurers to determine their relative
14 rights and obligations concerning the individual's entitlement or the amount or
15 kind of insurance benefits, when the policy of insurance insurer with respect to a
16 claim for benefits, or (8) between insurers and reinsurers in connection with the
17 underwriting and administration of coverages and the processing of claims.

18 The release or transfer of confidential medical information under any of the
19 above exceptions shall not be the basis for any legal liability, civil, or criminal, nor
20 considered a violation of this Act.

21 (c) Third parties receiving and retaining an individual's confidential health
22 care information must establish at least the following security procedures: (1) limit
23 authorized access to personally identifiable confidential health care information to
24 persons having a "need to know" such information; additional employees or agents
25 may have access to such information which does not contain information from
26 which an individual can be identified; (2) identify as individual or individuals who
27 have responsibility for maintaining security procedures for confidential health care
28 information; (3) provide a written statement to each employee or agent as to the
29 necessity of maintaining the security of confidential health care information, and of
30 the penalties provided for in this Act for the unauthorized release, use, or disclo-
31 sures of such information; receipt of such statement shall be acknowledged by such

-4-

1 employee or agent signing and returning same to his employer or principal and the
2 employer or principal shall furnish his employee or agent with a copy of the signed
3 statement, and shall retain the original thereof; (4) take no disciplinary or punitive action
4 against any employee or agent who brings evidence of violation of this Act to the atten-
5 tion of any person or entity.

6 (d) Consent forms for the release or transfer of confidential health care information
7 shall contain, or in the course of an application or claim for insurance be accompanied by
8 a notice containing, at least the following:

- 9 (1) the need for and proposed use of such information;
- 10 (2) a statement indicating specifically the type and extent of information to
11 be released, and
- 12 (3) a statement that such information will not be given, sold, transferred, or
13 in any way relayed to any other person or entity not specified in the
14 consent form or notice without first obtaining the individual's additional
15 written consent on a form stating the need for the proposed new use of
16 such information of the need for its transfer to another person or entity,
17 and,
- 18 (4) a statement that such consent applies only to the release or transfer of
19 confidential health care information existing prior to the date such con-
20 sent is signed, except that when such consent is given in the course of an
21 application or claim for insurance it shall also apply to medical informa-
22 tion existing at any time during the period of contestability provided for
23 in the policy and during periods of ongoing proofs of loss during a claim.

24 (e) where confidential health care information is in computer-retrievable form, such
25 information shall be subject to the following minimum security measures:

- 26 (1) limit authorized access to such information through the establishment of
27 some form of security clearance available only to authorized persons;
- 28 (2) identify individual(s) responsible for maintaining security procedures;
- 29 (3) any contracts with third parties shall, at a minimum, place no limits on
30 the third party's liability for breaches of its obligations to keep confiden-
31 tial health care information in strict confidence.

1 **Section 5.** (a) Every health care provider shall, upon written request of any patient
2 who has received health care services from such provider, at the option of the health care
3 provider either permit such patient (or his authorized attorney) to examine and copy the
4 patient's confidential health care information or provide such patient (or his authorized
5 attorney) a summary of such information.

6 At the time of such examination, copying or provision of summary information,
7 the health care provider shall be reimbursed for reasonable expenses in connection with
8 furnishing such information.

9 (b) If in the professional judgment of the health care provider, it would be injuri-
10 ous to the mental or physical health of the patient to disclose certain confidential health
11 care information to the patient, the health care provider is not required to disclose or
12 provide a summary of such information to the patient, but shall upon written request of
13 the patient (or his authorized attorney) disclose such information to another health care
14 provider designated by the patient.

15 (c)(1) Upon occurrence of an action or decision of any third party which adversely
16 affects a person, and which is based in whole or in part upon his confidential health care
17 information, including, but not limited to, the following actions:

- 18 • denial of an application for an insurance policy;
- 19 • issuance of an insurance policy with other than standard and
20 uniform restrictions;
- 21 • rejection in whole or in part of any claim for insurance benefits;
- 22 • denial of an employment application or termination of
23 employment when such denial or termination is for health
24 reasons;

25 and upon the written request of such persons or his authorized attorney or physician (or,
26 if such person is deceased, then his heir or beneficiary or their authorized representative
27 or his estate), a third party shall transfer all of person's confidential healthcare informa-
28 tion in its possession to such person's authorized attorney.

29 Prior to making such transfer, a third party may require payment of its cost of
30 retrieval, duplication and forwarding of such information.

1 (2) After reviewing his confidential health care information pursuant to this Sec-
2 tion, a person or his authorized attorney may request the third party to amend or expunge
3 any part he believes is in error, or request the addition of any recent relevant information.

4 Upon receiving such a request, the third party shall notify the health care provider
5 who initially forwarded such information to the third party, and when such health care
6 provider concurs with such request, the third party shall return such information to that
7 health care provider for modification. Prior to making such return, a third party may
8 require payment of its cost of notice, duplication, and return of such information. Except
9 upon court order, the third party shall not modify such information. A person after
10 requesting and reviewing his confidential health care information shall have the right, in
11 any case, to place into the file a statement of reasonable length of his view as to the
12 correctness or relevance of existing information or as to the addition of new information.
13 Such statement or copies thereof shall at all times accompany that part of the information
14 in contention.

15 **Section 6.** (a) (1) Except as provided in subparagraph (2) hereof, confidential
16 health care information shall not be subject to compulsory legal process in any type of
17 proceeding, including, but not limited to, any civil or criminal case or legislative or
18 administrative proceedings or in any pre-trial or other preliminary proceedings, and a
19 person or his authorized representative has a privilege to refuse to disclose, and to pre-
20 vent a witness from disclosing, his confidential health care information in any such
21 proceedings.

22 (2) The exemption from compulsory legal process and the privilege provided in
23 subparagraph (1) above shall not apply when:

24 (a) an individual introduces his physical or mental condition
25 including, but not limited to, any allegation of mental anguish,
26 mental suffering or similar condition as an element of his claim or
27 defense, provided that a claim for damages or other relief for "pain and
28 suffering" based solely on one's physical condition does not constitute the
29 introduction of one's mental condition into issue and the exemption and
30 privilege shall apply in such situation as to those portions of one's confiden-
31 tial health care information relating to mental condition;

-7-

- 1 (b) the individual's physical or mental condition is relevant regarding the
2 execution or witnessing of a will or other document;
- 3 (c) the physical or mental condition of a deceased individual is introduced by
4 any party claiming or defending through or as a beneficiary of such indi-
5 vidual;
- 6 (d) in a civil or criminal commitment proceeding, a physician, in the course
7 of diagnosis, treatment, or medical evaluation of an individual, determines
8 that an individual is in need of care and treatment in a hospital or any other
9 health care facility which is deemed by the individual's physician to be
10 appropriate for mental illness;
- 11 (e) a judge finds that an individual, after having been informed that the
12 communications would not be privileged, has made communications to a
13 psychiatrist in the course of a psychiatric examination ordered by the court,
14 provided that such communications shall be admissible only on issues in-
15 volving the individual's mental condition;
- 16 (f) in any court proceeding, including an ex parte hearing, it is demonstrated
17 on a prima facie basis to the court that the individual's physical or mental
18 condition is of an imminent and serious danger to the physical or mental
19 health of another person, or to the security of the United States; or
- 20 (g) in any action by an individual pursuant to Section 9 of this Act, or in
21 any policy action brought by an individual against his insurance carrier, or
22 by the carrier an insured, or in any other action by an individual wherein it
23 is demonstrated to the court that such confidential health care information
24 is relevant and material then such court may issue an order compelling
25 production of such information.

26 (b) the exceptions contained in items (A) through (G) of subparagraph (2) above
27 are not intended to preclude the exemption or privilege described in subparagraph (1)
28 above in any pretrial or trial proceedings under the Divorce Act of this State unless the
29 individual or witness on his behalf first testifies as to such confidential health care
30 information.

1 **Section 7.** (a) Notwithstanding other provisions of this Act, health care providers
2 may make confidential health care information available to medical peer review commit-
3 tees without authorization.

4 (b) Confidential health care information before a medical peer review committee
5 shall remain strictly confidential, and any person found guilty of the unlawful disclosure
6 of such information shall be subject to the penalties provided in this Act.

7 (c) Except as otherwise provided in this Section, the proceedings and records of
8 medical peer review committees shall not be subject to discovery or introduction into
9 evidence. No person who was in attendance at a meeting of such committee shall be
10 permitted or required to testify as to any matters presented during the proceedings of
11 such committee or as to any findings, recommendations, evaluations, opinions or other
12 actions of such committee or any members thereof.

13 Confidential health care information otherwise discoverable or admissible from
14 original sources is not to be construed as immune from discovery or use in any proceed-
15 ing merely because they were presented during proceedings before such committee, nor
16 is a member of such committee or other person appearing before it to be prevented from
17 testifying as to matters within his knowledge and in accordance with the other provisions
18 of this Act, but the said witness cannot be questioned about his testimony or other pro-
19 ceedings before such committee or about opinions formed by him as a result of said
20 committee hearings.

21 (d) The provisions of sub-section (c) above limiting discovery or testimony do not
22 apply in any legal action brought by a medical peer review committee to restrict or
23 revoke a physician's hospital staff privileges, or his license to practice medicine, or to
24 cases where a member of the medical peer review committee or the legal entity which
25 formed such a committee or within such committee operates is used for actions taken by
26 such committee, provided that in any such legal action personally identifiable portions of
27 a person's confidential health care information shall not be used without written authori-
28 zation of such person or his authorized representative or upon court order.

29 (e) Nothing in this Act shall limit the authority, which may otherwise be provided
30 by law, of a physician licensing or disciplinary board of this State to require a medical

1 peer review committee to report to it any disciplinary actions or recommendations of
2 such committee, or to transfer to it records of such committee's proceedings or actions,
3 including confidential medical information, or restrict or revoke a physician's license to
4 practice medicine, provided that an any such legal action personally identifiable
5 portions of a person's confidential health care information shall not be used without
6 authorization of such person or his authorized representative or upon court order.

7 (f) No member of a medical peer review committee nor the legal entity which
8 formed or within which such committee operates nor any person providing information
9 to such committee shall be criminally or civilly liable for the performance of any duty,
10 function, or activity of such committee or based upon providing information to such
11 committee; provided such action is without malice and is based upon a reasonable belief
12 that such action is warranted.

13 **Section 8. (a) Civil Penalties -** Anyone who violates provisions of this Act may be
14 held liable for special and general damages.

15 (b) **Criminal Penalties -** Anyone who intentionally and knowingly violates provi-
16 sions of this Act shall, upon conviction, be fined not more than \$1,000, or imprisoned for
17 not more than six months, or both.

18 (c) The civil and criminal penalties above shall also be applicable to anyone who
19 obtains an individual's confidential health care information through the commission of a
20 crime.

21 **Section 9.** A person or his authorized representative shall have the right, when
22 there is an unreasonable refusal to change the records as provided in Section 5, to seek
23 through court action the amendment or expungement of any part of his confidential
24 health care information in a third party's possession which he believes is erroneous.

25 **Section 9.1** To the extent a minor has the right under the laws of this state to
26 obtain health care services without the consent of a parent or guardian, such minor shall
27 have all rights under this Act relating to confidential health care information regarding
28 such health care services.

29 **Section 10.** Attorney's fees and reasonable costs may be awarded, at the discretion
30 of the court, to the successful party in any action under
31 this Act.

1 **Section 11.** Any agreement purporting to waive the provisions of this Act is hereby
2 declared to be against public policy and void.

3 **Section 12.** If any provision of this Act is held by a court to be invalid, such invalidity
4 shall not affect the remaining provisions of this Act, and to this end the provisions of this Act are
5 hereby declared severable.

6 **Section 13.** This Act shall become effective ____ (one year from the date of being signed
7 into law.)

1992

CODE OF MEDICAL ETHICS
CURRENT
OPINIONS

OF THE
**COUNCIL ON
ETHICAL AND JUDICIAL
AFFAIRS**

OF THE
**AMERICAN
MEDICAL
ASSOCIATION**



before releasing such information. The patient's decision is final under the law. Physicians are ethically and legally required to protect the personal privacy and other legal rights of patients. The physician-patient relationship and its confidential nature must be maintained. With these considerations in mind, the physician may assist the representatives of the media in every way possible. (IV)

-
- 5.05 **CONFIDENTIALITY.** The information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree. The patient should feel free to make a full disclosure of information to the physician in order that the physician may most effectively provide needed services. The patient should be able to make this disclosure with the knowledge that the physician will respect the confidential nature of the communication. The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law.

The obligation to safeguard patient confidences is subject to certain exceptions which are ethically and legally justified because of overriding social considerations. Where a patient threatens to inflict serious bodily harm to another person and there is a reasonable probability that the patient may carry out the threat, the physician should take reasonable precautions for the protection of the intended victim, including notification of law enforcement authorities. Also, communicable diseases, gun shot and knife wounds should be reported as required by applicable statutes or ordinances. (IV)

-
- 5.06 **CONFIDENTIALITY: ATTORNEY-PHYSICIAN RELATION.** The patient's history, diagnosis, treatment, and prognosis may be discussed with the patient's lawyer with the consent of the patient or the patient's lawful representative.

A physician may testify in court or before a worker's compensation board or the like in any personal injury or related case. (IV)

-
- 5.07 **CONFIDENTIALITY: COMPUTERS.** The utmost effort and care must be taken to protect the confidentiality of all medical records. This ethical principle applies to computerized medical records as it applies to any other medical records.

The confidentiality of physician-patient communications is desirable to assure free and open disclosure by the patient to the physician of all information needed to establish a proper diagnosis and attain the most desirable clinical outcome possible. Protecting the confidentiality of the personal and medical information in such medical records is also necessary to prevent humiliation, embarrassment, or discomfort of patients. At the same time, patients may have legitimate desires to have medical information concerning their care and treatment forwarded to others.

Both the protection of confidentiality and the appropriate release of information in records is the rightful expectation of the patient. A physician should respect the patient's expectations of confidentiality concerning medical records that involve the patient's care and treatment, but the physician should also respect the patient's authorization to provide information from the medical record to those whom the patient authorizes to inspect all or part of it for legitimate purposes.

Computer technology permits the accumulation, storage, and analysis of an unlimited quantum of medical information. The possibility of access to information is greater with a computerized data system than with information stored in the traditional written form in a physician's office. Accordingly, the guidelines below are offered to assist physicians and computer service organizations in maintaining the confidentiality of information in medical records when that information is stored in computerized data bases. It should be recognized that specific procedures adapted from application of these concepts may vary depending upon the nature of the organization processing the data as well as the appropriate and authorized use of the stored data.

Guidelines on a computerized data base.

- (1) Confidential medical information entered into the computerized data base should be verified as to authenticity of source.
- (2) The patient and physician should be advised about the existence of computerized data bases in which medical information concerning the patient is stored. Such information should be communicated to the physician and patient prior to the physician's release of the medical information. All individuals and organizations with some form of access to the computerized data bank, and the level of access permitted, should be specifically identified in advance.
- (3) The physician and patient should be notified of the distribution of all reports reflecting identifiable patient data prior to distribution of the reports by the computer facility. There should be approval by the physician and patient prior to the release of patient-identifiable clinical and administrative data to individuals or organizations external to the medical care environment, and such information should not be released without the express permission of the physician and the patient.
- (4) The dissemination of confidential medical data should be limited to only those individuals or agencies with a bona fide use for the data. Release of confidential medical information from the data base should be confined to the specific purpose for which the information is requested and limited to the specific time frame requested. All such organizations or individuals should be advised that authorized release of data to them does not authorize their further release of the data to additional individuals or organizations.

- (5) Procedures for adding to or changing data on the computerized data base should indicate individuals authorized to make changes, time periods in which changes take place, and those individuals who will be informed about changes in the data from the medical records.
- (6) Procedures for purging the computerized data base of archaic or inaccurate data should be established and the patient and physician should be notified before and after the data has been purged. There should be no commingling of a physician's computerized patient records with those of other computer service bureau clients. In addition, procedures should be developed to protect against inadvertent mixing of individual reports or segments thereof.
- (7) The computerized medical data base should be on-line to the computer terminal only when authorized computer programs requiring the medical data are being used. Individuals and organizations external to the clinical facility should not be provided on-line access to a computerized data base containing identifiable data from medical records concerning patients.
- (8) Security:
 - A. Stringent security procedures for entry into the immediate environment in which the computerized medical data base is stored and/or processed or for otherwise having access to confidential medical information should be developed and strictly enforced so as to prevent access to the computer facility by unauthorized personnel. Personnel audit procedures should be developed to establish a record in the event of unauthorized disclosure of medical data. A roster of past and present service bureau personnel with specified levels of access to the medical data base should be maintained. Specific administrative sanctions should exist to prevent employee breaches of confidentiality and security procedures.
 - B. All terminated or former employees in the data processing environment should have no access to data from the medical records concerning patients.
 - C. Involuntarily terminated employees working in the data processing environment in which data from medical records concerning patients are processed should immediately upon termination be removed from the computerized medical data environment.
 - D. Upon termination of computer service bureau services for a physician, those computer files maintained for the physician should be physically turned over to the physician, or destroyed (erased). In the event of file erasure, the computer service bureau should verify in writing to the physician that the erasure has taken place (IV).

5.08 CONFIDENTIALITY: INSURANCE COMPANY REPRESENTATIVE. History, diagnosis, prognosis, and the like acquired during the physician-patient relationship may be disclosed to an insurance company representative only if the patient or a lawful representative has consented to the disclosure. A physician's responsibilities to patients are not limited to the actual practice of medicine. They also include the performance of some services ancillary to the practice of medicine. These services might include certification that the patient was under the physician's care and comment on the diagnosis and therapy in the particular case. (IV)

5.09 CONFIDENTIALITY: PHYSICIANS IN INDUSTRY. Where a physician's services are limited to pre-employment physical examinations or examinations to determine if an employee who has been ill or injured is able to return to work, no physician-patient relationship exists between the physician and those individuals. Nevertheless, the information obtained by the physician as a result of such examinations is confidential and should not be communicated to a third party without the individual's prior written consent, unless it is required by law. If the individual authorized the release of medical information to an employer or a potential employer, the physician should release only that information which is reasonably relevant to the employer's decision regarding that individual's ability to perform the work required by the job.

A physician-patient relationship does exist when a physician renders treatment to an employee, even though the physician is paid by the employer. If the employee's illness or injury is work-related, the release of medical information as to the treatment provided to the employer may be subject to the provisions of workers compensation laws. The physician must comply with the requirements of such laws, if applicable. However, the physician may not otherwise discuss the employee's health condition with the employer without the employee's consent or, in the event of the employee's incapacity, the family's consent.

Whenever statistical information about employees' health is released, all employee identities should be deleted. (IV)

Socioeconomic
Characteristics of
Medical Practice
1993

Studies on the Socioeconomic Environment of Medicine

Electronic Billing of Physician Services
by Anita J. Chawla

Physician Profiling
by David W. Emmons and Gregory D. Wozniak

Physician Involvement with Alternative Delivery Systems
by Kurt D. Gillis and David W. Emmons

Socioeconomic Characteristics of Allergy/Immunology Practice
by Sara L. Thurán

Physician Earnings, 1981-1991
by James W. Moser

Medical Professional Liability Claims and Premiums, 1985-1991
by Martin L. Gonzalez

Electronic Billing of Physician Services

by Anita J. Chawla

Reducing the level and growth rate of health expenditures has become a primary goal of most health system reform proposals. While there is considerable debate on the extent to which administrative costs contribute to health care cost inflation, most policy analysts would acknowledge that streamlining the administration of health care services would provide at least a one-time reduction in administrative costs. It has been suggested that one area in which administrative cost savings could be achieved is the billing for providers' services and submission of insurance claims. The application of electronic transmission of data, bills, and claims between providers and third-party payers could be one source of administrative cost savings.

Administrative Costs and Electronic Billing

Promotion of electronic billing and claims submission as a means to reduce administrative costs has received increased attention since the publication of the Workgroup for Electronic Data Interchange (WEDI) report to the Secretary of the Department of Health and Human Services in July 1992. The WEDI report was a product of a private sector initiated workgroup convened in response to Secretary Sullivan's challenge to industry to address the reduction of administrative costs. In addition to reviewing the state of electronic data interchange in the health care industry, the WEDI report proposed objectives and an action plan to foster widespread adoption of electronic data interchange within the next five years.

Currently, electronic claims submission is far more prevalent for Medicare services. The Health Care Financing Administration estimates that close to 80% of claims for hospital services and 45% for physician services are submitted electronically. The percentage of providers submitting claims electronically in the Medicaid program varies from state to state, with as few as 35% of physicians and as many as 90% of hospitals using electronic claims submission in some states. Blue Cross and Blue Shield estimates that among its plans, more than half of hospital claims (79% of Medicare Part A claims and 60% of private sector hospital claims) are transmitted electronically. Electronic submission of claims for physician services is less than for hospital services with only 50% of Medicare Part B and 20% of private sector physician claims submitted through electronic data interchange. There is a much lower incidence of electronic data interchange in claims submission among commercial carriers. It is estimated that, in 1991, only about 10% of commercial indemnity claims were submitted electronically.

Electronic Claims Capability in Physician Offices, 1991 and 1992

The American Medical Association has recently begun to collect information on physicians' electronic billing capability in their practices using the Socioeconomic Monitoring System (SMS) survey. Results that characterize electronic billing activity in physician offices from the 1991 and 1992 core sur-

Table 1. Electronic Claims Submission in Physician Offices, 1991-1992*

	1991	1992
Percentage of physicians whose practices submit claims and have electronic billing capability	42.2%	49.0%
Percentage of physicians who treat Medicare patients whose practices submit Medicare claims electronically	28.7	38.1
Percentage of physicians who treat non-Medicare patients whose practices submit non-Medicare claims electronically	21.9	29.6

Source: See text of article.

* The differences between 1991 and 1992 are statistically significant ($p < .01$).

veys are presented in this report.² The results presented here are derived from a sample of physicians who practiced at least some fee-for-service medicine. Physicians responding to the SMS survey were asked if their practices submit insurance claims directly to third-party carriers. Those who submitted claims directly were asked if their practices had the capability to submit insurance claims to third-party carriers electronically. While SMS survey data on physician office electronic billing is thus far only available for the years 1991 and 1992, the data indicate that physicians are increasingly choosing to acquire the capability to submit claims electronically. The percentage of physicians who submit claims directly to third-party carriers and whose practices have the capability of billing claims electronically increased from 42.2% to 49.0% between 1991 and 1992.

Physicians who submitted claims directly and had electronic billing capability were asked if they submitted claims electronically to Medicare and non-Medicare carriers. Among Medicare providers (services provided in the last 12 months) with electronic billing capability, the percentage of physicians who submitted Medicare claims electronically increased from 28.7% to 38.1%. During the same period, among physicians who provided services to non-Medicare patients and had electronic billing capability, the percentage that electronically submitted claims to non-Medicare carriers increased

Table 2. Percentage of Physicians Who Submit Claims Directly to Third-Party Carriers and Whose Practices Have Capability of Billing Claims Electronically, by Selected Characteristics, 1992

All Physicians	49.0
<i>Specialty^a</i>	
General Family Practice	44.0
Medical Specialties	52.0
Surgical Specialties	51.0
Other Specialties	47.0
<i>Region^a</i>	
Northeast	47.0
North Central	48.0
South	44.0
West	42.0
<i>Location^a</i>	
Nonmetropolitan	52.0
Metropolitan less than 1,000,000	52.0
Metropolitan 1,000,000 and over	49.0
<i>Employment Status</i>	
Employee	51.5
Self-Employed	48.1
<i>Practice Size^a</i>	
Solo Practice	26.3
Two Physician Practice	42.4
Three Physician Practice	49.0
4-8 Physician Practice	51.5
Over 8 Physician Practice	70.0
<i>Age^a</i>	
Less than 40 years	52.0
40-45	51.0
46-55	51.4
56-65	43.5
More than 66	28.7

Source: See text of article.

*Differences are statistically significant ($p < .01$).

from 21.9% to 29.6%. The increases in electronic billing capabilities during the 1991 to 1992 period, detailed in Table 1, are all statistically significant ($p < .01$).

Electronic Claims Capability in Physician Offices, 1992

Table 2 shows the percentage of physicians who have the capability of billing claims electronically across a variety of physician characteristics. Over

50% of physicians in medical and surgical specialties have such a capability. Physicians in specialties other than general family practice, medical and surgical specialties are the least likely to have electronic billing capability. Physicians who have electronic billing capability are more likely to be located in the south than in other regions, and they are more likely to be located in nonmetropolitan areas. Nearly 55% of physicians in the south had electronic billing capability compared with only 40% in the northeast. Physicians in large metropolitan areas are far less likely to have electronic billing capability (44.1%) than those in nonmetropolitan areas (56%).

There are distinct differences in electronic billing capabilities according to employment status and practice size. Only 48% of self-employed physicians, compared with 52% of employee physicians, have electronic billing capability in their practice. The relationship between practice size and billing capability is even more dramatic. Physicians in large practices are far more likely to have electronic billing capability. In practices with more than eight physicians, 70% reported having the capability to bill electronically. Among those in solo practice, only 36% reported having electronic capability. The cost of acquiring the hardware and software required for electronic claims submission is a significant obstacle for smaller practices and for physicians who are not employees. In smaller practices, the costs are likely to be spread among few physicians while in large group practices physicians may not directly bear the costs of acquiring electronic data interchange technology. Furthermore, in smaller practices it is less likely that non-physician office staff would be familiar with electronic data interchange; costs associated with training personnel also represent a significant obstacle to implementing electronic claims transmission. Thus, electronic claims submission may not be cost effective for a number of physician practices, particularly those that are small.

Younger physicians are most likely to have electronic billing capability in their practices. Fifty-three percent of physicians under 40 years of age reported having a capability. Among physicians over 66 years of age, only 29% indicated their practices did so.

The likelihood that a physician would have electronic billing capability would be expected to vary according to the proportion of services provided to

Table 3 Percentage of Physicians Who Submit Claims Directly to Third-Party Carriers and Whose Practices Have Capability of Billing Claims Electronically, by Percent of Revenues from Selected Third-Party Payers, 1992

All Physicians	40.2*
<i>Percentage of Revenue from Medicare^a</i>	
0-10%	40.2
11-25%	41.3
26-40%	47.4
More than 40%	42.5
<i>Percentage of Revenue from Blue Cross/Blue Shield^b</i>	
0-10%	40.2
11-25%	40.4
26-40%	48.2
More than 40%	45.7
<i>Percentage of Revenue from Other Payers^c</i>	
0-10%	50.7
11-25%	50.0
26-40%	49.2
More than 40%	41.3

Source: See text of article.

*Differences are statistically significant ($p < .01$).

^bDifferences are statistically significant ($p < .01$).

patients with different health insurance coverage. Electronic data interchange for claims submission has been promoted most aggressively by HCFA for reimbursing providers for Medicare services. The SMS data shown in Table 3 indicate that the greater the percentage of a physician's revenue from Medicare, the more likely the physician is to have electronic billing capability. Slightly less than 57% of physicians with over 40% of their practice revenue derived from Medicare have electronic capability in their practice. Only 36% of those with 10% or less of their revenue from the provision of Medicare services have electronic billing capability.

The percentage of physicians having electronic capability varies with the percentage of revenue from Blue Cross and Blue Shield. While these variations are statistically significant, the relationship between the proportion of revenue and the likelihood of having this capability is not as clear as is for revenue from Medicare. For example, physicians who receive more than 40% of their revenue from Blue Cross and Blue Shield (BCBS) are less likely to have electronic billing capability than those receiving 11-25% and 26-40% of their revenue

Table 4 Percentage of Physicians Who Provided Services to Medicare Patients in the Last 12 Months that Submitted Claims to Medicare Electronically, 1992

	Percent
All Physicians	38.1
<i>Specialty^a</i>	
General Family Practice	38.1
Medical Specialties	41.2
Surgical Specialties	39.3
Other Specialties	31.1
<i>Region^a</i>	
Northeast	30.1
North Central	41.8
South	42.7
West	34.9
<i>Location^a</i>	
Nonmetropolitan	47.4
Metropolitan less than 1,000,000	41.6
Metropolitan 1,000,000 and over	32.2
<i>Employment Status</i>	
Employee	41.1
Self-Employed	37.2
<i>Practice Size^a</i>	
Solo Practice	25.5
Two Physician Practice	33.8
Three Physician Practice	45.1
4-8 Physician Practice	52.6
Over 8 Physician Practice	62.1
<i>Age^a</i>	
Less than 40 years	40.5
40-45	40.9
46-55	41.9
56-65	31.7
More than 66	19.7

Source: See text of article.

^aDifferences are statistically significant ($p < .01$).

^bDifferences are statistically significant ($p < .05$).

Table 5 Percentage of Physicians Who Provided Services to Non-Medicare Patients in the Last 12 Months that Submitted Claims to Non-Medicare Carriers Electronically, 1992

	Percent
All Physicians	20.7
<i>Specialty</i>	
General Family Practice	15.2
Medical Specialties	20.1
Surgical Specialties	17.8
Other Specialties	24.4
<i>Region^a</i>	
Northeast	22.1
North Central	17.4
South	12.2
West	28.2
<i>Location^a</i>	
Nonmetropolitan	39.7
Metropolitan less than 1,000,000	31.0
Metropolitan 1,000,000 and over	24.4
<i>Employment Status^a</i>	
Employee	36.7
Self-Employed	27.5
<i>Practice Size^a</i>	
Solo Practice	16.7
Two Physician Practice	26.9
Three Physician Practice	42.3
4-8 Physician Practice	57.7
Over 8 Physician Practice	54.6
<i>Age^a</i>	
Less than 40 years	32.2
40-45	30.4
46-55	33.3
56-65	24.4
More than 66	14.5

Source: See text of article.

^aDifferences are statistically significant ($p < .01$).

from BCBS, but are about as likely to have a capability as physicians with 0-10% of their revenue from BCBS.

Electronic Claims Submission of Medicare and Non-Medicare Claims, 1992

Table 4 shows the likelihood of electronic claims submission of Medicare claims for Medicare provid-

ers with electronic data interchange capability. In 1992, 38.1% of Medicare providers who could submit claims electronically from their offices did so. The incidence of electronic claims submission among physicians who provided non-Medicare services and could submit claims electronically was much lower (Table 5).

Among physicians who provided Medicare services those in medical specialties were more likely to

Table 6 Proportion of Medicare and Non-Medicare Claims Submitted Electronically, 1992

	1-25%	26-50%	51-75%	76-100%
Percentage of physicians submitting Medicare claims in this proportion (among physicians who treat Medicare patients)	44	28	7	85
Percentage of physicians submitting Non-Medicare claims in this proportion (among physicians who treat Non-Medicare patients)	31.9	23.2	12.4	32.4

Source: See text of article.

submit claims electronically than physicians in general/family practice, surgical, or other specialties. The percentage of physicians who provided non-Medicare services and electronically submitted claims to non-Medicare carriers did not vary significantly according to specialty.

For both Medicare and non-Medicare providers who submitted claims electronically, there were statistically significant differences, among regions, locations, and practice sizes, in the percentage of physicians submitting claims electronically. The patterns of variation are somewhat different. For Medicare providers, physicians in the south and nonmetropolitan areas were more likely to submit claims electronically. Among those providing non-Medicare services, a greater percentage of physicians located in the north central region and nonmetropolitan areas submitted claims electronically to non-Medicare carriers. In general, for both Medicare and non-Medicare providers, physicians in larger practices were more likely to submit claims electronically. The relationship between practice size and the likelihood of submitting claims electronically is particularly strong for Medicare providers submitting Medicare claims.

The use of electronic claims submission in physician offices is more widespread for Medicare services than for non-Medicare services. Table 6 shows that, among physicians who submitted claims electronically to Medicare, 86% submitted between 76% and 100% of their Medicare claims electronically. Physicians who treated non-Medicare

patients submitted smaller shares of their non-Medicare claims electronically. Only one-third of these physicians submitted 76-100% of their non-Medicare claims electronically, nearly the same percentage submitted 1-25% of their non-Medicare claims.

In part, the difference in the extent to which physicians use electronic claims submission for Medicare and non-Medicare claims probably reflects higher implicit costs associated with electronic data interchange with non-Medicare carriers. In addition to actively promoting electronic claims submission for Medicare services, HCFA has standardized the format for submission. There is a myriad of submission formats among private sector third-party payers, and physicians argue that the multiplicity of formats contributes to the "hassle factor" of practicing medicine.

1. All figures presented in this section are from the Report to Secretary of U.S. Department of Health and Human Services (Washington, D.C. Workgroup for Electronic Data Interchange) July 1992.

2. Some data on electronic billing from the SAS 1991 core survey have been presented in American Medical Association Center for Health Policy Research, "Electronic Billing of Insurance Claims for Physician Services," *Physician Marketplace* (Issue 3) (March 1992).

Mr. CONDIT. Mr. Entin.

**STATEMENT OF FREDRIC ENTIN, SENIOR VICE PRESIDENT
AND GENERAL COUNSEL, AMERICAN HOSPITAL ASSOCIATION**

Mr. ENTIN. Thank you, Mr. Chairman, and I, too, appreciate the opportunity to appear before you today.

I am Fred Entin, I am senior vice president and general counsel of the American Hospital Association. The AHA is a voluntary membership organization of over 5,300 institutions, primarily hospitals. We have been seriously addressing the complex question of health care reform for several years, and we believe we have provided constructive, credible input in the Nation's debate over reform.

The AHA believes that the goals of universal coverage and control of costs cannot be achieved unless the system is fundamentally restructured. As the chairman is no doubt aware, our current system is complicated, its problems are many, and there is no single solution to reform.

There will be a need for a whole host of measures, the sum total of which will contribute to the transformation of this system into one which provides all Americans high quality, efficient care. Electronic automation of the vast amounts of information that exist in health care offers much to achieve cost-effective care. The AHA vision of a reformed health care delivery system is based around community based health networks that integrate financing and delivery of care. To make these networks function well, we must take advantage of the latest information technology to make health care better coordinated and user friendly.

For better coordination of care to occur in a network structure, information must be able to move across time, across many sites and many providers of care. If we're able to do that, the payoff will be administrative simplification and better care. Improved electronic information infrastructure must be installed, therefore, to support efforts to pull together a current system that is fragmented and highly inefficient.

Inherent in network formation is the aggregation of individual provider and payer information systems into larger shared information networks. Data in such shared networks would be efficiently or effectively directed to health care practitioners, hospital and health care administrators, payers, purchasers, quality and utilization reviewers, and researchers, enabling all to respond to the pressures that are driving the call for health care reform right now.

It is critical that we apply new technology to make it possible for data to be directed in ways not previously thought possible. Of course, the ease of data transmission carries with it a risk, that of unauthorized disclosure.

The same technology that so easily moves and stores information makes confidentiality—confidential information much more vulnerable to disclosure.

We commend the chairman for his efforts in H.R. 4077 to strike the appropriate balance between the need to apply the latest in data technology to health care reform, and at the same time to ensure that the integrity of records containing sensitively confidential information of the most private details of our lives is safeguarded.

We are in general agreement with the principles in the bill, and the standards set forth in the bill establish a framework that should be uniformly applied.

We have a number of suggestions that we believe will strengthen the bill and they are set forth in our written testimony. We believe that these suggestions would better enable you to achieve the goals that the bill seeks to achieve, and I'd like to talk about a couple in my oral remarks.

First, I'd like to address the question of preemption, Mr. Chairman. In the findings and purposes section of the bill, there are two important observations: First is that in our current system the legal protections for confidentiality vary greatly from State to State.

The second observation is that movement of individuals and health care information across State lines and the emergence of multistate providers and payers, creates a compelling need for a uniform Federal law, and rules and procedures governing the use, maintenance, and disclosure of information. We agree with those observations and suggest that the argument for Federal preemption is compelling.

All of the attributes of our current confusing, unduly complicated system must be simplified. What we're operating under right now is a patchwork of inconsistent, conflicting and, in many cases, inadequate State laws. Some State laws in fact prohibit the use of computerized patient records requiring orders in ink. Others require the storage media to be original paper.

Other State laws do not address a patient's right to see, copy or correct their medical record, and some State laws fail to set forth obligations of those who come in contact with private information in order to safeguard that confidentiality. What we have right now is a system that promotes confusion and makes it difficult to protect confidentiality. Today we waste resources due to this system, resources which could be better deployed to take care of patients.

To transform the system into a rational, efficient delivery system, we must have a single set of standards and laws. There is no justification, given the multistate nature of care and payment, for the maintenance of 50 State approaches to the problem.

Federal legislation should set forth a single standard. No State should have the option to provide more or less protection. There must be preemption and we offer to work with the subcommittee to draft such a clause for the bill.

Second, just as preemption is necessary to eliminate the complexity of the current system, the goal of any such legislation should be to simplify the issue so as to make it easier for legitimate users of patient information to comply with the law. Respectfully, we suggest that we should reexamine the approach in the bill which defines different types of users to identify the different obligations to use and disclose individually identifiable information.

Instead of making it clearer to legitimate users of protected health information, we are concerned that the use of the three-trustee concept will prove to be confusing and impose complicated burdens. For example, it's possible that an individual may fit into different trustee categories in a single day, or even at the same

time. It's possible an individual may not fit into any category and thus be unclear as to what his responsibilities are.

The duties of the "affiliated person" found in the bill further complicate the process. Rather than assign responsibilities according to the category a user might fit into, we recommend a single standard of confidentiality to apply to all individually identifiable information. This sets forth a single standard which, first, respects the constitutional underpinnings of privacy; and second, tells all users what their responsibilities are when in possession of individually identifiable information.

To address those circumstances where public policy would authorize disclosure, certain explicit exceptions could be defined so that close family members, law enforcement agencies, public health officials and the like, may have immediate access to necessary information. And I note that in the bill many of those exceptions are already contained.

We believe having limited exceptions designed around the use of information is a more workable approach and ultimately one that will be less confusing than the trustee concept found in the bill.

We commend the chairman for H.R. 4077. We believe it is the appropriate step at this stage of the Nation's health care debate to address the fundamental tensions between two legitimate competing principles. H.R. 4077 strikes the right balance between the priorities of using electronic data to help restructure the health care system, and the rights of all Americans to reasonable guarantees of privacy.

Thank you for the opportunity to address the committee, and I welcome any questions.

Mr. CONDIT. Thank you, Mr. Entin.

[The prepared statement of Mr. Entin follows:]

American Hospital Association



Capitol Place, Building #3
50 F Street, N.W.
Suite 1100
Washington, D.C. 20001
Telephone 202 638-1100
FAX NO 202 626-2345

**Testimony
of the
American Hospital Association
before the
Information, Justice, Transportation, and Agriculture Subcommittee
of the
Committee on Government Operations
of the
United States House of Representatives
on
Confidentiality of Health Care Records**

May 4, 1994

Mr. Chairman, I am Fredric J. Entin, Senior Vice President and General Counsel of the American Hospital Association (AHA). On behalf of the AHA's 5,300 institutional members, I am pleased to comment on H.R. 4077, the Fair Health Information Practices Act of 1994.

The Need to Promote the Health Information Infrastructure

This country is on the verge of comprehensive health reform. We hope, as we work to reform the nation's health care delivery system, that we will emerge with a system of community-based health networks that integrate the financing and the delivery of care. We believe that by bringing providers together into health networks, we will provide incentives to integrate services and coordinate care, yielding more efficient and appropriate utilization of precious health care resources.

to integrate services and coordinate care, yielding more efficient and appropriate utilization of precious health care resources.

A health information infrastructure is central to our vision of an integrated delivery system. By such an infrastructure, we mean an interconnected communication network capable of linking all participants in the U.S. health system. For better coordination of care to occur, information about patients must move smoothly across times, sites, and providers of care. Each health care facility and practitioner would connect to and become part of a larger shared information network. By increasing the accessibility of patient information, this electronic information infrastructure can help improve quality, increase efficiency, and control costs. When authorized, data from such a system could flow to health care managers, payers, purchasers, policy makers, and researchers to monitor the performance of the health care system and make key decisions for the future. However, because this information will be traveling through a variety of providers, payers and health data repositories, including processing vendors and clearinghouses, this information will become more vulnerable to unauthorized disclosures.

Current Problems

As we move toward our goal, we are faced with the challenge of finding an acceptable balance between providing greater access to health care information and protecting patient rights to privacy. For all the enthusiasm among those within the health care sector for migrating toward computerized information systems, many Americans view the

computerization of personal health information with suspicion, if not outright hostility. No obstacle to the development of this infrastructure looms larger than the public's concerns about safeguarding the flow of personal health information.

As we begin to build a nationwide information infrastructure, we have an obligation to examine the currently inconsistent laws and regulations which govern the exchange of patient information. Many state and federal laws create obstacles to legitimate sharing of health information that could yield better patient care, administrative savings, and more efficient patient management. For example, some states prohibit the use of computerized record systems by requiring that orders be written in ink, often referred to as the "quill pen" laws or by restricting the permissible health record storage media to the original paper or microfilm.

Moreover, payers and providers that operate in more than one state are required to comply with a multitude of different rules, which adds to administrative inefficiency. The burdensome and costly obligation of complying with individual--often inconsistent--state laws is obvious. Such costs add nothing to the quality of care and divert resources that could be better deployed.

Despite this plethora of state laws, most of which include some form of confidentiality protection, identifiable health care information still remains vulnerable to unauthorized disclosures. Furthermore, many state laws do not address key issues, like a patient's right to

see, copy, and correct his or her own records, and the obligations of anyone who comes in contact with individually identifiable health care information--including but not limited to, payers, providers, processing vendors, storage vendors and utilization review organizations--to protect confidentiality. As a result, the varying requirements of the current system promote confusion over confidentiality rights.

At the same time, because many of these state laws were written in the context of the paper records of yesterday, they frequently do not offer sufficient security for today's world of electronic data interchange (EDI). The shared information networks of the future will require explicit and uniform confidentiality requirements for handling health care data. Identifiable health care information traveling in an EDI environment is more vulnerable to unauthorized disclosures. Special protections need to be in place for this type of information in order to provide appropriate incentives for providers and payers to move toward EDI while assuring confidentiality. Therefore, a uniform federal law must ensure that individually identifiable health care information be maintained confidentially as it travels from place to place.

Solutions

AHA applauds your efforts, Mr. Chairman, in introducing H.R. 4077, the Fair Health Information Practices Act of 1994. AHA believes that it is crucial to focus on the issue of maintaining health care information in a confidential and private manner while this nation debates reform. In order to effectively restructure our health care delivery system,

information must be shared in an appropriate manner without sacrificing the confidential and private nature of such information.

Although AHA generally supports the principles contained in this bill, there are a number of points that AHA would like to address. These include: the concept of "Trustee" as outlined in the proposed legislation; equal protection for all individually identifiable health care information, regardless of its perceived sensitivity; federal preemption; and oversight authority.

The first area of concern relates to confusion with the "Trustee" concept, which has many different legal and financial connotations. Because the term Trustee may in fact imply more than the meaning intended in this bill, AHA suggests either making "Trustee" a better defined term or substituting a new word that might more accurately reflect the intent of the bill. The concept of three defined trustees is also a confusing and complicated method of assigning responsibility for respect to individually identifiable health care information. For example, it is possible that an individual may fit into multiple trustee categories simultaneously or even at different times during the day. It is also possible that an individual may not fit into any trustee category and therefore, may have no idea what, if any, responsibilities he/she has with regard to protecting health care information. Although, AHA understands that different individuals will come into contact with individually identifiable health care information for different purposes, we believe that regardless of the context, individually identifiable health care information deserves to be protected equally. AHA

would recommend that a simple and less confusing approach is to develop a single set of standards for all uses and users.

Similarly, all individually identifiable health care information should be protected equally. No special protection should be afforded to individually identifiable health care information which is perceived to be highly sensitive. Every individual should be granted the same protections, for what may not appear to be sensitive information to some, may in fact be quite sensitive to others. Additionally, whenever sensitive information is segregated for protection purposes it becomes obvious that the segregated information is more sensitive, therefore making that information even more vulnerable to leakage or unauthorized disclosure.

Perhaps one of the most important components of any proposed confidentiality legislation is the preemption section. AHA believes that in order to reap the benefits of electronic information exchange while still protecting patient privacy and confidentiality, there must be federal legislation to preempt state laws regarding the collection, storage, processing, and transmission of individually identifiable health care information. All personally identifiable health care information, regardless of where it originates or where it is transmitted should be handled under the direction of a uniform federal law. Additionally, federal law must create a system where confidentiality rights no longer vary from state to state--in other words the federal law should serve as both the "floor" and the "ceiling," such that no state could provide less protection or more protection.

Unfortunately, the bill fails to provide for federal preemption. We understand that you, Mr. Chairman, recognize the importance of preemption and we are anxious to work with you and your staff to draft the most comprehensive, complete and appropriate preemption clause.

Without such a clause this proposed legislation will not provide a uniform set of protections and rules for maintaining individually identifiable health care information confidentially and privately. If the proposed legislation is not uniform and complete, we will be maintaining the current patchwork of different State laws rather than having the protection of one uniform standard.

Finally, the agency or oversight authority which will promulgate regulations and administer this Act should not be the Department of Health and Human Services (HHS). Although this may appear to be the logical choice, HHS as a payor and administrator of health services would also be subject to the requirements of this Act. The dual role of regulator and the regulated appears to be a conflict of interest. The responsibility for implementing this Act should be assigned either to an existing or new administrative agency not otherwise responsible for administering or providing health care programs.

Principles Governing the Protection of Health Records

The issue of the protection of confidentiality of patient information is not a new one; rather, the government has been active in this arena for many years.

In 1973, the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems set out the following principles to govern electronic data systems.

- Existence of personal data record keeping systems must be identified and not kept secret;
- Individuals should be able to find out what information is in their records and how it is used;
- Individuals should be able to prevent information that was obtained for one purpose from being used or made available for other purposes without their consent;
- Individuals should be able to correct or amend a record of identifiable information;
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must take precautions to prevent misuse of the data.

The Office of Technology Assessment (OTA) recently submitted a report entitled "Protecting Privacy in Computerized Medical Information". This report states that the present system of protecting health care information offers a "patchwork of codes, state laws of varying scope, and Federal laws applicable to limited kinds of information." The OTA Report

concludes by stating that "the present legal scheme does not provide consistent, comprehensive, protection for privacy in health care information, and it is inadequate to guide the health care industry with respect to obligations to protect the privacy of medical information in a computerized environment." The OTA report concludes by stating that federal law is necessary to address issues of patient confidentiality and privacy.

In November 1991, HHS Secretary Sullivan convened a forum of national health care leaders to discuss the challenges of reducing administrative costs in the U.S. health care system. At the forum, several health care industry-led workgroups were created--including the Workgroup for Electronic Data Interchange (WEDI) and the Workgroup on Computerized Patient Records. Both of these Workgroups submitted reports to the Secretary recommending ways the health care industry could begin reducing administrative costs associated with the delivery of and payment for health care, and recommended that national standards be established for protecting the confidentiality of individually identifiable health care information. The American Hospital Association participated in both groups and strongly supports the recommendation that Congress enact federal preemptive legislation governing the confidentiality of individually identifiable health care information.

WEDI, a public/private partnership consisting of health care leaders from all segments of the health care delivery and payment communities, believes that national legal standards for the protection of the confidentiality of personal health information should:

- Establish uniform requirements for the preservation of confidentiality and privacy rights in electronic health care claims processing and payment;
- Address the collection, storage, handling and transmission of individually identifiable health care data, including initial and subsequent disclosures, in electronic transactions by all public and private payers, providers of health care, and all other entities involved in the transactions;
- Ensure that preemption will not supersede state public health reporting laws which address the particular health safety needs of a community;
- Delineate protocols for secure electronic storage and transmission of health care data;
- Specify fair information practices that ensure a proper balance between required disclosures, use of data, and patient privacy;
- Require publication of the existence of health care data banks;
- Encourage use of alternate dispute resolution mechanisms, where appropriate;
- Establish that compliance with the Act's requirements would serve as a defense to legal actions based on charges of improper disclosure;

- Impose penalties for violation of the Act, including civil damages, equitable remedies, and attorney's fees, where appropriate; and
- Provide enforcement by government officials and private, aggrieved parties.

WEDI reconvened in January 1993 and set up a Workgroup on Confidentiality/Legal Issues to draft model legislation. This model legislation is included in a report delivered to Secretary Shalala in November of 1993 and is attached to this statement. The requirements of this legislation are intended to apply to all entities, including public and private third-party payers and providers, that collect, store, process, or transmit such information in electronic form. The legislation would protect individually identifiable health care information, but would not affect federal and state laws that require reporting of identifiable information to public health authorities. It would also place oversight authority in an independent national privacy commission.

Conclusion

The American public is concerned about the development of a new health information system, where personal health information will easily travel through a variety of health repositories. Simultaneously, all individually identifiable health care information needs to be protected regardless of the medium. Although the future of health care will most likely be automated, all individually identifiable health care information deserves to be protected regardless of the medium. As we automate, the public must be assured that the benefits of

computerizing their health information substantially outweigh the potential risk of any unauthorized disclosures. AHA commends you, Mr. Chairman, for your efforts in drafting the Fair Health Information Practices Act of 1994. The steps you outline will do much to ensure the confidentiality and privacy of health care records and clinical encounters. AHA does not, however, believe that the intent of this proposed legislation is to unduly burden or cause mass confusion for the legitimate users of identifiable health care information. AHA is recommending therefore, that the "Trustee" concept as described in H.R. 4077 be reconsidered. The existence of so many different "rules" may in fact be an impediment to the effective protection of patient identifiable information. Instead of a framework which different standards exist for different circumstances, we recommend that all individually identifiable health care information be handled uniformly. Health care information is highly sensitive and should be treated in a uniform manner, regardless of the nature of the information.

AHA believes that it is essential that federal law occupy the field and completely preempt the application of state law to the collection, storage, processing and transmission of individually identifiable health care information. If our new health care system, in which many health providers will either deliver care or share information in multiple jurisdictions, is to protect unauthorized disclosures of individually identifiable health care information and preserve its privacy and confidentiality, comprehensive legislation must be enacted--at the same time as the enactment of the new health care system itself--that will ensure uniform and confidential treatment of identifiable health care information.

Finally, as this subcommittee contemplates the appropriate oversight agency, AHA continues to believe that an independent entity who is neither a payer, administrator, or provider of health care services would be important to the establishment of public confidence in a new health delivery environment. We do not believe it is possible for HHS to reconcile the conflict of interest that occurs when it serves as both the regulated and the regulator.

We appreciate the opportunity to present our views to this subcommittee and look forward to working with you as the issues of reform and confidentiality move forward.

**ATTACHMENT
AMERICAN HOSPITAL ASSOCIATION TESTIMONY
MAY 4, 1994**

Addenda

**Addendum 1: Text of Proposed "Health Information
Confidentiality and Privacy Act of 1993"**

MODEL FEDERAL LEGISLATION

CONFIDENTIALITY OF ELECTRONIC HEALTH CARE INFORMATION

A BILL

To provide for the preservation of confidentiality and privacy rights in the collection, storage, processing and transmission of individually identifiable health care information (including initial and subsequent disclosure) in electronic form; to preempt state laws relating thereto, except public health reporting laws; to establish a regulatory mechanism for delineating protocols for securing electronic collection, storage, processing, and transmission of such health care information, and for fair information practices; to require publication of the existence of health care data banks; to encourage the use of alternative dispute resolution mechanisms, where appropriate, for resolving disputes arising under this Act; and to establish penalties for violation.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1 - SHORT TITLE

This Act may be cited as the "Health Information Confidentiality and Privacy Act of 1993."

SECTION 2 - SCOPE

- A. **Applicability.** This Act shall apply to the collection, storage, processing, and transmission of individually identifiable health care information (including initial and subsequent disclosures) in electronic form by all persons, including but not limited to public and private third-party payors and providers of health care.

- B. Protection. The protections of this Act shall extend to individuals who are the subject of individually identifiable health care information that is collected, stored, processed or transmitted in electronic form.
- C. Exemptions. This Act shall not apply to federal or state laws or regulations that require reporting of individually identifiable health care information to public health authorities.

SECTION 3 - DEFINITIONS

For purposes of this Act:

- A. "Disclosure" includes the initial release and any subsequent redisclosures of individually identifiable health care information.
- B. "Electronic form" means all mechanical, non-paper formats, including fiberoptic transmission and laser disc storage.
- C. "External Disclosure(s)" means:
 - (1) All disclosures of individually identifiable health care information to person(s) who are not employed or credentialed by, or who do not have an independent contractor relationship with a payor or provider; and
 - (2) Which are made on behalf of the individual and are directly related to either the adjudication of a claim, coordination of benefits, or to the medical treatment of an individual.
- D. "Health care" means:
 - (1) Any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service or procedure provided by a provider:
 - (a) with respect to an individual's physical or mental condition; or
 - (b) affecting the structure or function of the human body or any part thereof, including, but not limited to, banking of blood, sperm, organs, or any other tissue; and
 - (2) The prescription, sale or dispensing of any drug, substance, device, equipment, or other item to an individual or for an individual's use for health care.

- E. "Individual" means a natural person who is the subject of individually identifiable health care information, and includes the individual's legal representative.
- F. "Individually identifiable health care information" means any data or information that identifies or can reasonably be associated with the identity of an individual, either directly or by reference to other publicly available information, and:
 - (1) Relates to the individual's health history, health status, health benefits, or application therefor; or
 - (2) Is obtained in the course of an individual's health care from a provider, from the individual, from a member of the individual's family, or from a person with whom the individual has a close personal relationship.
- G. "Person" means a government, governmental subdivision, agency or authority, natural person, corporation, estate, trust, partnership, association, joint venture, and any other legal entity.
- H. "Provider" means a person that is duly authorized, or that represents itself as being duly authorized to provide health care.
- I. "Secretary" means . . .

SECTION 4 - PREEMPTION

Unless otherwise provided in Section 2 C, upon the effective date of regulations implementing this Act, no effect shall be given to any provision of state law that requires individually identifiable health care information to be maintained exclusively in written rather than electronic form or to any provision of state law to the extent it relates to the matters covered in this Act, including the preservation of confidentiality and privacy rights in the collection, storage, processing, and transmission of individually identifiable health care information (including initial and subsequent disclosures) in electronic form by all involved in such transactions.

SECTION 5 - STANDARDS FOR INFORMATION PRACTICES

- A. The Secretary shall, by regulation, establish appropriate levels of security, standards, and controls including but not limited to passwords, access codes, restrictions on access, limitations on networking and electronic data sharing, and protocols and procedures for preventing computer sabotage, for collecting, storing, processing and transmitting individually identifiable health care information in electronic form so as to ensure the

privacy and confidentiality of such information, taking into consideration the nature of the information and relative risks of disclosure.

- B. The regulations promulgated pursuant to Section 5 A shall incorporate the following principles:
 - (1) The individual shall have the right to know that individually identifiable health care information concerning the individual is collected, stored, processed or transmitted by any person, and to know for what purpose such information is used.
 - (2) Individually identifiable health care information shall be collected, processed, stored and transmitted only to the extent necessary to carry out a legitimate purpose for which the individual has granted consent.
 - (3) Each person collecting individually identifiable health care information from an individual shall notify the individual or his or her right to receive a statement, in the style and form prescribed by the Secretary, summarizing the individual's rights pursuant to this Act.
 - (4) The individual shall have a right of access to individually identifiable health care information concerning the individual from the person collecting such information, the right to have a copy of such information after payment of a reasonable charge, and the right to have a notation made with or in such information of any amendment or correction requested by the individual.
 - (5) Persons collecting, processing, storing or transmitting individually identifiable health care information shall implement or cause to be implemented as the case may be, the appropriate security standards and controls promulgated by the Secretary to assure the accuracy, reliability, relevance, completeness, timeliness and security of such information.

SECTION 6 - DISCLOSURE

- A. Disclosure. Except as authorized in Section 6 D, no person other than an individual shall disclose individually identifiable health care information to any other person without the individual's valid authorization as provided in Section 6 C. No person shall disclose such information except in accordance with the terms of such authorization, unless otherwise authorized under Section 6 D.

- B. **Record or Disclosures.** Each person collecting or storing individually identifiable health care information shall maintain a record of all external disclosures made on behalf of a provider, in favor of individual, or such information.
- C. **Individual Authorization: Requirements for Validity.**
- (1) To be valid, an authorization to disclose individually identifiable health care information must –
 - (a) Identify the individual;
 - (b) Describe the health care information to be disclosed;
 - (c) Identify the person to whom the information is to be disclosed;
 - (d) Describe the purpose of the disclosure;
 - (e) Indicate the length of time for which the individual's authorization will remain valid;
 - (f) Be either,
 - (i) In writing, dated and signed by the individual; or
 - (ii) In electronic form, dated and authenticated by the individual using a unique identifier; and
 - (g) Not have been revoked under Section 6 C (2).
 - (2) **Revocation of Individual's Authorization.** An individual may revoke the individual's authorization at any time, unless disclosure is required to effectuate payment for health care that has been provided to the individual, or other action has been taken in reliance on the individual's authorization. An individual may not maintain an action against a person for disclosure of individually identifiable health care information made in good faith reliance on the individual's authorization, provided the disclosing person had no notice of the revocation of the individual's authorization at the time disclosure was made.
 - (3) **Record of Individual's Authorizations and Revocations.** Each person collecting or storing individually identifiable health care information shall maintain a record of each individual's authorization and revocation thereof, and such record shall become part of the

individually identifiable health care information concerning such individual.

- (4) **No Waiver.** Except as provided by this Act, an authorization to disclose individually identifiable health care information by an individual is not a waiver of any rights an individual has under other federal or state statutes, the rules of evidence, or common law.

D. Disclosure Without An Individual's Authorization. A person may disclose individually identifiable health care information without the individual's authorization required in Section C if:

- (1) The disclosure is by a family member or by any other person with whom the individual has a close personal relationship, unless such disclosure is expressly limited or prohibited by the individual;
- (2) The disclosure is only to the extent necessary for the disclosing person to carry out its lawful activities and is to the disclosing person's agent, employee, or independent contractor who is under an obligation to hold the individually identifiable health care information in confidence and not to use such information for any purpose other than the lawful purpose for which the information was obtained by the disclosing person;
- (3) The disclosure is to a provider who is providing health care to the individual except as such disclosure is limited or prohibited by the individual;
- (4) The disclosing person reasonably believes that disclosure is necessary to avoid or minimize imminent danger to the health or safety of any individual, but only to the extent necessary to avoid or minimize such danger or emergency;
- (5) The disclosure is to a member of the individual's immediate family, or to any other individual with whom the patient is known to have a close personal relationship, if such disclosure is made in accordance with good medical or other professional practice, unless such disclosure is expressly limited or prohibited by the individual;
- (6) The disclosure is to a successor in interest to the person maintaining the individually identifiable health care information, provided, however, that no person other than a provider or the estate of a deceased provider shall be considered a successor in interest to a provider;

- 7) The disclosure is to federal, state, or local government authorities, to the extent the person providing the individually identifiable health care information is required by law to report specific individually identifiable health care information:
 - (a) when needed to determine compliance with state or federal licensure, certification, or registration rules or laws; or
 - (b) when needed to protect the public health;
- 8) The disclosure is to a person solely for purposes of conducting an audit, if that person agrees in writing:
 - (a) to remove or destroy, at the earliest opportunity consistent with the purpose of the audit, information that would enable identification of the individual;
 - (b) not to disclose in any report any individually identifiable health care information; and
 - (c) not to further disclose the information, except to accomplish the audit or to report unlawful or improper conduct involving health care fraud by a provider or the individual or other unlawful conduct by a provider;
- 9) The disclosure is for use in a research project that:
 - (a) is of sufficient importance to outweigh any potential harm to the individual that would result from the disclosure;
 - (b) is reasonably impracticable without the use of the individually identifiable health care information;
 - (c) contains reasonable safeguards to protect the information from redisclosure;
 - (d) contains reasonable safeguards to protect against identifying, directly or indirectly, any individual in any report of the research project;
 - (e) contains procedures to remove or destroy at the earliest opportunity, consistent with the purposes of the project, information that would enable identification of the individual, unless retention of identifying information is required for purposes of another research project that also satisfies the requirements of this Section; and

- (9) The person agrees in writing:
 - (i) to remove or destroy, at the earliest opportunity consistent with the purpose of the research information that would enable identification of the individual;
 - (ii) to not disclose individually identifiable health care information, except as necessary to conduct the research project;
- (10) The disclosure is in accordance with a discovery request:
 - (a) Before service of a discovery request on a person maintaining individually identifiable health care information, an attorney shall provide advance notice to the person and to the individual involved or the individual's representative or attorney through service of process or first class mail, indicating what information is sought, and the date by which a protective order must be obtained to prevent the person from complying. Such date shall give the individual and the person adequate time to seek a protective order, but in no event be less than fourteen days after the date of service of such notice;
 - (b) Without the individual's authorization, a person may not disclose the information sought under paragraph (a) if the requestor has not complied with the requirements of paragraph (a). In the absence of a protective order issued by a court of competent jurisdiction forbidding compliance, the person shall disclose the information in accordance with this section. In the case of compliance, the request for discovery or compulsory process shall be maintained by the holder thereof with the individual's health care information;
 - (c) Production of individually identifiable health care information under this section, in and of itself, does not constitute a waiver of any privilege, objection, or defense existing under other law or rule of evidence or procedure;
- (11) The disclosure is to federal, state or local law enforcement authorities to the extent required or permitted by law;
- (12) The disclosure is directed by a court in connection with a court-ordered examination of an individual; or

- 3) The disclosure is based on reasonable grounds to believe that the information is needed to assist in the identification of a deceased individual.

E. Obligations of Legal Representatives

- 1) A person authorized to act as an individual's legal representative may exercise the rights of the individual under this Act to the extent necessary to effectuate the terms or purposes of the grant of authority; but an individual who is a minor and who is authorized to consent to health care without the consent of a parent or legal guardian under state law may exclusively exercise the rights of an individual under this Act as to information pertaining to health care to which the minor lawfully consented.
- 2) An individual's legal representative shall act in good faith to represent the best interests of the individual with respect to individually identifiable health care information.

SECTION 7 - PUBLICATION

Persons collecting individually identifiable health care information shall, pursuant to regulations, periodically publicize the existence of the information and provide information regarding procedures for obtaining and correcting the information.

SECTION 8 - AMENDMENT OF INDIVIDUALLY IDENTIFIABLE HEALTH CARE INFORMATION

- A. Within thirty (30) business days from the date of receipt of a written request from an individual to amend any individually identifiable health care information about the individual within its possession, a person collecting, storing or processing such information shall either:
- (1) Amend the portion of the recorded individually identifiable health care information identified by the individual, or
 - (2) Notify the individual of:
 - a) Its refusal to make such amendment;
 - b) The reasons for the refusal, and

- (C) The individual's right to file a statement as provided in Subsection 8C.
- B. If the person amends information in accordance with Subsection 8 A above, the person shall provide the amendment to:
- (1) The individual;
 - (2) Any person specifically designated by the individual who may have, within the preceding two (2) years, received such information;
 - (3) Other persons who have systematically been provided such information within the preceding seven (7) years; provided, however, that the amendment or fact or deletion need not be furnished if the other person no longer maintains such information about the individual; and
 - (4) Any person that provided the information that has been amended.
- C. Whenever an individual disagrees with a person's refusal to amend individually identifiable health care information, the individual shall be permitted to file with such person:
- (1) A concise statement setting forth what the individual believes to be correct, relevant or fair information; and
 - (2) A concise statement of the reasons why the individual disagrees with the refusal to amend such information.
- D. If an individual files either statement as described in Subsection C above, the person shall:
- (1) Include the statement with the disputed individually identifiable health care information and provide a means by which anyone reviewing such information will be made aware of the individual's statement and have access to it;
 - (2) With any subsequent disclosure of the information that is the subject of disagreement, clearly identify the matter or matters in dispute and provide the individual's statement along with the information being disclosed; and
 - (3) Provide the statement to the persons and in the manner specified in Subsection 8 B above.

- E. The rights granted in this section shall not apply to individually identifiable health care information that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving the individual.

SECTION 9 - ALTERNATIVE DISPUTE RESOLUTION

The Secretary shall promulgate regulations that will promote the resolution of disputes arising under this Act through alternative dispute resolution mechanisms.

SECTION 10 - PROMULGATION OF REGULATIONS

- A. In promulgating regulations under this Act, the Secretary shall follow the procedures authorized under the "Negotiated Rulemaking Act of 1990," 5 U.S.C. §§ 581-590.
- B. If the Secretary determines that a negotiated rulemaking committee shall not be established as permitted by 5 U.S.C. § 583, the Secretary shall appoint and consult with an advisory group of knowledgeable individuals. The advisory group shall consist of at least seven (7) but no more than twelve (12) individuals from the following areas: (1) health care financing and reimbursement; (2) health care delivery, including representatives of health care professionals and health care entities; (3) third party payors/administrators, network administrators; and (4) health care consumers.
- C. The advisory group shall review all proposed rules and regulations and submit recommendations to the Secretary. The advisory group shall also assist the Secretary: (1) in establishing the standards for compliance with rules and regulations; and (2) in developing an annual report to the Congress on the status of the requirements set forth in this Act, their cost impact, and any recommendations for modifications in order to ensure efficient and confidential electronic data interchange of individually identifiable health care information.

SECTION 11 - CIVIL REMEDIES

- A. An individual aggrieved by a violation of this Act may maintain an action for relief as provided in this section.
- B. The district courts of the United States shall have exclusive jurisdiction in any action brought under the provisions of this section.

- C. The court may order a person maintaining individually identifiable health care information to comply with this Act and may order any other appropriate relief.
- D. If the court determines that there has been a violation of this Act, the aggrieved individual shall be entitled to recover damages for any losses sustained as a result of the violation; and, in addition, if the violation results from willful or grossly negligent conduct, the aggrieved individual may recover not in excess of \$10,000, exclusive of any loss.
- E. If an aggrieved individual prevails in an action brought under this section, the court, in addition to any other relief granted under this section, may award reasonable attorneys' fees and all other expenses incurred by the aggrieved individual in the litigation.
- F. Any action under this Act must be brought within two years from the date on which the alleged violation is discovered.

SECTION 12 - CIVIL MONEY PENALTIES

Any person that knowingly discloses health care information in violation of this Act shall be subject, in addition to any other penalties that may be prescribed by law -

- A. to a civil money penalty of not more than \$10,000 for each violation, but not to exceed \$50,000 in the aggregate for multiple violations; and, in addition -
- B. to a civil money penalty of not more than \$100,000 if the Secretary finds that violations of this Act have occurred with such frequency as to constitute a general business practice.

SECTION 13 - IMMUNITY

It shall be an affirmative defense in actions brought for improper disclosure of individually identifiable health care information that such disclosure was in accordance with the requirements of this Act and regulations promulgated pursuant to this Act.

SECTION 14 - CRIMINAL PENALTIES FOR OBTAINING INDIVIDUALLY IDENTIFIABLE HEALTH CARE INFORMATION THROUGH FALSE PRETENSES OR THEFT

- A. Any person who, under false or fraudulent pretenses, requests or obtains individually identifiable health care information shall be fined not more than \$50,000 or imprisoned not more than six months, or both, for each offense.
- B. Any person who unlawfully takes, or under false or fraudulent pretenses, requests or obtains individually identifiable health care information and who intentionally uses, sells or transfers such information for remuneration, for profit or for monetary gain shall be fined not more than \$100,000, or imprisoned for not more than two years, or both, for each offense.

SECTION 15 - SEVERABILITY

If any provision of this Act or its application to any person or circumstance is held invalid, it shall not affect other provisions or applications of this Act that can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

SECTION 16 - EFFECTIVE DATE

Except as provided in Section 4, this Act shall become effective upon enactment.

Mr. CONDIT. Mr. Gimpel.

STATEMENT OF JOEL E. GIMPEL, ASSOCIATE GENERAL COUNSEL, BLUE CROSS AND BLUE SHIELD ASSOCIATION, CHICAGO, IL, REPRESENTING THE WORKGROUP ON ELECTRONIC DATA INTERCHANGE

Mr. GIMPEL. Mr. Chairman, and members of the subcommittee, I am Joel Gimpel, associate general counsel of the Blue Cross and Blue Shield Association, which is the coordinating organization for the 69 independent Blue Cross and Blue Shield plans operating in the United States and Puerto Rico.

I am testifying here today, however, as a representative of the Workgroup on Electronic Interchange, or WEDI, having served as the cochair of WEDI's technical advisory group on confidentiality and legal issues. I am pleased to present WEDI's views on Federal legislation governing the confidentiality of identifiable health care information in general, and on H.R. 4077 in particular.

In my oral testimony today, I would summarize the principal points of my written submission. I intend to provide an overview of WEDI's efforts to date, to outline WEDI's principles for privacy protection legislation, note our consideration of the Privacy Act of 1974, and comment on H.R. 4077, noting WEDI's concerns with certain of its provisions.

WEDI was established in November 1991, to reduce administrative costs in the Nation's health care system. It is a voluntary public and private task force and it developed an action plan to streamline health care administration by standardizing electronic communications across the industry. I might add parenthetically, Mr. Chairman, that all of the members sitting at this panel had representatives of their sponsoring or their employing entities serving on WEDI's 25-member steering committee.

In July 1992, WEDI published a report to the HHS Secretary of the steps it felt necessary to make electronic data interchange routine for the health care industry by 1996. Those 1992 recommendations dealt with such issues as the need for standard formats for four core financial transactions, phased implementation by the industry, and the creation of incentives for increased use of EDI.

They also dealt with the need for unique identifiers and various other technical issues. In addition, the 1992 WEDI report recommended that Congress enact Federal preemptive legislation to facilitate and assure the uniform confidential treatment of identifiable information in electronic environments. The confidentiality and legal issues technical advisory group which developed that recommendation approached the issue with a desire to facilitate achieving WEDI's overall objective of moving to an EDI environment for health care transactions by 1996. And to accomplish that goal, the group believed it necessary to remove statutory impediments such as "quill pen" laws, and other laws that inhibit or prevent the use of EDI for health care transactions.

Several proposals were discussed, including the development of a model State law for adoption by all States within 3 years. To state that proposal, however, is to discard it as probably not being feasible, for we considered it most unlikely that all States would adopt uniform privacy legislation in the foreseeable future.

The group also considered proposing a Federal law that sets standards for State legislation, but allows States to adopt more stringent standards. This too was rejected because of the need to establish a uniform regulatory environment.

Accordingly, the group decided that the only logical course was to recommend enactment of Federal preemptive legislation governing confidentiality that would completely occupy the field.

WEDI reconvened in 1993 to resolve implementation obstacles and work toward engaging all of the health care trading partners in standardized automation and electronic communication.

In November 1993, WEDI released its second report. With particular respect to the section in that report regarding confidentiality and legal issues, it includes proposed Federal legislation that is designed to preserve confidentiality and privacy rights in health care information; to preempt State laws that relate thereto, except for public health reporting laws; to establish a mechanism for promulgating regulations that delineate protocols for securing information; to require publication of the existence of health care data banks; to encourage the use of alternative dispute resolution mechanisms to resolve certain disputes that arise; and to establish penalties for violating the act.

Mr. Chairman, although complete copies of the 1992 and 1993 reports submitted by WEDI to HHS were furnished to all Members of the Congress, I have attached copies of the 1993 executive summary and report of the confidentiality and legal issues technical advisory group, which does include the text of WEDI's proposed legislation, to my prepared testimony.

What are WEDI's principles for privacy protection? We are encouraged by the obvious interest shown by many Members of the Congress in general, and this subcommittee in particular, in developing appropriate privacy protections and encouraging migration to electronic data interchange in the health care system.

In evaluating legislation in this area, we believe, however, that certain principles should be recognized and that Federal privacy legislation must: completely preempt State laws, except public health reporting laws that inhibit the use of EDI by our health care industry; protect identifiable health care information wherever located and however obtained; designate an impartial regulator to administer and enforce the law; and establish appropriate standards for privacy and confidentiality protection.

And to that end, Mr. Chairman, the WEDI proposal sets forth five principles that have to be—that should be incorporated in regulations that establish security standards. They are: No. 1, guarantee the individual's right to know that identifiable health information is being collected and stored and processed and for what purpose it's used.

No. 2, assure that the information is collected, processed, stored and transmitted only as required for a legitimate purpose.

No. 3, the rules should require that persons collecting information notify individuals of their rights under the act.

No. 4, the rules should guarantee an individual's right of access to information from the person collecting the information.

And No. 5, the rules should require that persons collecting, storing, processing, or transmitting identifiable information implement

the standards and controls that are promulgated by the regulatory agency.

WEDI's principles for legislation also call for rapid implementation. The legislation should be uncomplicated and enforceable. And, of course, should provide appropriate civil and criminal penalties for violation.

Before commenting on H.R. 4077, I believe it appropriate to comment on the possibility of expanding the application of the Privacy Act of 1974 to nongovernmental entities. That possibility, too, was considered and rejected by WEDI's confidentiality and legal issues technical advisory group for several reasons. First, an extensive rewrite would be required to apply the Privacy Act's provisions to nongovernmental entities, and a preemption provision would have to be engrafted. Most importantly, however, the act's structure is inappropriate for application to private industry in that, for instance, it authorizes agency heads to promulgate rules to exempt any system of records within the agency from certain of the act's requirements, and to promulgate rules regarding procedures for examining records.

Nevertheless, WEDI drew upon many of the concepts contained in the Privacy Act's provisions regarding conditions of disclosure, accounting for certain disclosures, access to records and others in drafting its proposed legislation.

Let me provide a few comments on H.R. 4077. We are honored to have been asked to contribute to the development of the bill, and WEDI representatives have met on many occasions with your staff and others to discuss the various issues dealt with in the legislation.

We believe that our overall objectives and philosophies are compatible, but are concerned with respect to certain of the provisions in H.R. 4077. First and foremost of those concerns is the absence of a provision preempting State laws that deal with privacy of identifiable health care information, because the absence of a sufficient preemption provision will result in uneven privacy protection, and thereby inhibit if not prevent universal implementation of electronic data interchange for health care transactions.

We're also concerned that H.R. 4077 doesn't appear to apply to identifiable health care information in a nontreatment setting. In other words, information regarding health status in applications for life insurance and employment would not be protected and could be disclosed.

Our third principal concern is that the bill would not become effective until January 1, 1997, which could unduly delay the universal implementation of electronic data interchange in our health care system. We also have an overriding concern regarding the possible complications and opportunity for game playing that may arise from the three-trustee arrangement contemplated in the bill.

In order to be enforceable, those regulated by the act must know with reasonable certainty what regulations and requirements they must follow. Because, however, a given entity may at any time be a health-use trustee, a public-health trustee, and a special-purpose trustee, depending upon the specific set of circumstances, it would be difficult if not impossible to assure that it was complying with the right set of rules.

Furthermore, entities that fall into more than one class of trustee would have to establish different sets of controls to protect privacy in different transactions. We would therefore urge careful examination of the trustee concept to explore whether it could be simplified and to carefully consider alternative solutions to the problem.

Those solutions might include establishment of only two trustee categories, for example, health-use trustees which should include employers and others that maintain health-related information in nonpatient settings, and special-purpose trustees, exempting certain users from certain of the act's requirements.

We also note that H.R. 4077 assigns to the Secretary of Health and Human Services the responsibility for administering and enforcing the act. This may be inappropriate in that the Department of Health and Human Services would itself be regulated under the act. For that reason, we urge that consideration be given to assigning enforcement and administrative responsibility to an independent governmental agency that is neither a health care provider nor payer.

In conclusion, Mr. Chairman, WEDI believes that in order to make possible the many benefits of universal electronic data interchange in health care transactions, the health care industry, including private and public payers, providers and vendors of information services, must be able to travel the information superhighway without having to consider 51 different rules of the road for privacy protection.

WEDI also urges that privacy protection is warranted for identifiable health care information obtained in nonpatient settings, and that the responsibility for administering and enforcing Federal privacy legislation be assigned to an agency that is not itself a health care provider or payer.

Furthermore, WEDI has recommended five principles for privacy protection that should be incorporated in security standards.

Finally, we urge that legislation be uncomplicated and enforceable, provide appropriate penalties for violation, and be implemented as soon as possible.

We look forward to working with your committee and with the Congress to develop meaningful and appropriate legislation that facilitates the universal implementation of EDI in health care, while protecting the privacy rights of individuals.

I believe that H.R. 4077 represents an important first step toward that goal.

Thank you for your attention and I'll be happy to answer any questions you may have.

Mr. CONDIT. Thank you, Mr. Gimpel.

[The prepared statement of Mr. Gimpel follows:]

TESTIMONY OF THE
WORKGROUP ON ELECTRONIC DATA INTERCHANGE
ON
CONFIDENTIALITY OF INDIVIDUALLY IDENTIFIABLE
HEALTH CARE INFORMATION

BEFORE THE
INFORMATION, JUSTICE, TRANSPORTATION, AND AGRICULTURE SUBCOMMITTEE
OF THE
COMMITTEE ON GOVERNMENT OPERATIONS
U.S. HOUSE OF REPRESENTATIVES

BY
JOEL E. GINPEL
ASSOCIATE GENERAL COUNSEL
BLUE CROSS AND BLUE SHIELD ASSOCIATION

APRIL 27, 1994

INTRODUCTION

Mr. Chairman and Members of the Subcommittee:

I am Joel Gimpel, Associate General Counsel of the Blue Cross and Blue Shield Association, which is the coordinating organization for the 69 independent Blue Cross and Blue Shield Plans operating in the United States and Puerto Rico. I am testifying here today as a representative of the Workgroup on Electronic Data Interchange, or WEDI, having served as the co-chair of WEDI's Technical Advisory Group on confidentiality and legal issues. I am pleased to present WEDI's views on federal legislation governing the confidentiality of individually identifiable health care information in general, and on HR 4077, the Fair Health Information Practices Act of 1994, in particular.

In my testimony today, I will:

- Provide an overview of WEDI's efforts to date;
- Outline WEDI's principles for privacy protection legislation;
- Note WEDI's consideration of the Privacy Act of 1974; and
- Comment on HR 4077, noting WEDI's concerns with certain provisions.

OVERVIEW OF WEDI'S EFFORTS

WEDI was established in November 1991, in response to a challenge from Dr. Louis Sullivan, then Secretary of the Department of Health and Human Services, to reduce administrative costs in the nation's health care system. WEDI, which is a voluntary, public-private task force, developed an action plan to streamline health care administration by standardizing electronic communications across the industry.

In July 1992, WEDI published a report to the Secretary of the steps it felt necessary to make electronic data interchange routine for the health care industry by 1996. The 1992 recommendations dealt with such issues as the need for standard formats for four core financial transactions, phased implementation by industry of WEDI for those core transactions, the creation of incentives by public and private payers and the Congress for increased use of EDI, the use of standardized billing content for claim submissions, the need for a unique identifier system that covers all participants in the health care system, and

WEDI TESTIMONY

Page 2

various other technical issues. In addition, the 1992 WEDI report recommended that Congress enact federal preemptive legislation to facilitate and assure the uniform, confidential treatment of identifiable information in electronic environments.

The Confidentiality and Legal Issues Technical Advisory Group, which developed that recommendation, approached the issue with the desire to facilitate the achievement of WEDI's overall objective of moving to an EDI environment for health care transactions by 1996. To accomplish that goal, the group believed it necessary to remove statutory impediments such as "quill-pen" and other laws that inhibit or prevent the use of EDI for health care transactions. Several proposals were discussed, including the development of a model state law for adoption by all states within three years. To state the proposal, however, is to discard it as not being feasible, for we considered it most unlikely that all states would adopt uniform privacy legislation in the foreseeable future.

The technical advisory group also considered proposing a federal law that sets standards for state legislation, but allows states to adopt more stringent standards. This, too, was rejected because of the need to establish a uniform regulatory environment. Accordingly, the group decided that the only logical course was to recommend the enactment of federal preemptive legislation governing confidentiality that would completely occupy the field.

WEDI reconvened in 1993 to resolve remaining implementation obstacles and work toward engaging all health care trading partners in standardized automation and electronic communication. The membership of WEDI's steering committee was expanded to include 26 national organizations representing payers, providers, consumers, federal and state health care governmental agencies, and businesses. Over 200 people representing all areas of the health care industry served in 11 technical advisory groups.

In November 1993, WEDI released its second report, which contained recommendations regarding standards implementation and uniform data content, network architecture and accreditation, confidentiality and legal issues, unique identifiers, education and publicity, health care identification cards, short term strategies, state and federal roles, financial implications, coordination of benefits, and health care fraud prevention and detection.

WEDI TESTIMONY

Page 3

With particular respect to the section regarding confidentiality and legal issues, the report includes proposed federal legislation designed to:

- preserve confidentiality and privacy rights in individually identifiable health care information that is collected, stored, processed or transmitted in electronic form;
- preempt state laws that relate thereto, except public health reporting laws;
- establish a mechanism for promulgating regulations that delineate protocols for securing such information when collected, stored, processed or transmitted in electronic form and that set forth fair information practices;
- require publication of the existence of health care data banks;
- encourage the use of alternative dispute resolution mechanisms to resolve certain disputes under the Act; and
- establish penalties for violating the Act.

To these ends, WEDI intends that the Act be construed so as to broadly protect individually identifiable health care information from improper and unauthorized disclosures in an electronic environment, while facilitating the prompt and universal implementation of electronic data interchange for legitimate and necessary health care transactions.

Although complete copies of WEDI's 1992 and 1993 reports were furnished to all members of the Congress, I've attached copies of the 1993 Executive Summary and report of the Confidentiality and Legal Issues Technical Advisory Group, which includes the text of WEDI's proposed legislation, to my prepared testimony.

PRINCIPLES FOR PRIVACY PROTECTION

We are encouraged by the obvious interest shown by many members of the Congress in general, and this subcommittee in particular, in developing appropriate privacy protections and encouraging migration to electronic data interchange in the health care system. In evaluating legislation in this area, however, we believe that certain principles should be recognized and that federal privacy legislation must:

WEDI TESTIMONY

Page 4

- Completely preempt state laws, except public health reporting laws, that inhibit the use of electronic data interchange by our health care industry and relate to the preservation of privacy and confidentiality of identifiable health care information. WEDI believes that complete preemption is required in order to provide uniform rules of the road regarding privacy protection for all travelers on the health care information superhighway.
- Protect identifiable health care information wherever located and however obtained. WEDI believes that identifiable health care information obtained in non-patient settings, such as employment and insurance applications, merits similar protection against unauthorized disclosure.
- Designate an impartial regulator to administer and enforce the law. WEDI is concerned that enforcement by a federal agency that is itself a health care provider or health care payer could lead to problems.
- Establish appropriate standards for privacy and confidentiality protection. To that end, the WEDI proposal sets forth five principles to be incorporated in regulations that establish security standards.

They are:

1. Guarantee the individual's right to know that identifiable health care information is collected, stored, processed, and for what purpose it is used,
 2. Assure that the information is collected, processed, stored, and transmitted only as required for a legitimate purpose;
 3. Require that persons collecting information notify individuals of their rights under the Act;
 4. Guarantee an individual's right of access to information from the person collecting the information;
 5. Require persons collecting, processing, storing, or transmitting identifiable information to implement the standards and controls promulgated by the regulatory agency.
- Provide for rapid implementation. WEDI believes that, to realize the benefits from universal use of electronic data interchange in the

WEDI TESTIMONY

Page 5

health care system as soon as possible, it is necessary to have in place appropriate and uniform rules for protecting the privacy of individuals.

- Be uncomplicated and enforceable. Although we recognize that no legislation is perfect, unnecessarily complicated legislation will make enforcement and implementation difficult.
- Provide appropriate civil and criminal penalties. WEDI believes that penalties for violations must be sufficient in order to foster compliance, yet not so high as to inhibit their imposition, and that the penalties suggested in the WEDI proposal, both civil and criminal, achieve the necessary balance.

CONSIDERATION OF THE PRIVACY ACT OF 1974 (5 USC § 552a)

Before commenting on HR 4077 as introduced by Congressman Condit, I believe it appropriate to comment on the possibility of expanding the application of the Privacy Act of 1974 to non-governmental identities. That possibility was considered and rejected by WEDI's Confidentiality and Legal Issues Technical Advisory Group for several reasons. First, an extensive rewrite would be required to apply the Privacy Act's provisions to non-governmental entities, and a preemption provision would have to be engrafted. Most importantly, however, the Act's structure is inappropriate for application to private industry in that, for instance, it authorizes agency heads to promulgate rules to exempt any system of records within the agency from certain of the Act's requirements and to promulgate rules regarding procedures for examining records. Nevertheless, WEDI drew upon many of the concepts contained in the Privacy Act's provisions regarding conditions of disclosure, accounting for certain disclosures, access to records, and others, in drafting its proposed legislation.

COMMENTS ON HR 4077

WEDI is honored to have been asked to contribute to the development of HR 4077, and WEDI representatives have met on many occasions with staff of this committee to discuss the various issues dealt with in the legislation. We believe that our overall objectives and philosophies are compatible, but are concerned with respect to certain of the provisions in HR 4077, which concerns have been brought to the attention of committee staff in prior discussions.

WEDI TESTIMONY

Page 6

First and foremost of those concerns is the absence of a provision preempting state laws (other than laws regarding public health reporting) that deal with privacy of identifiable health care information. The absence of a sufficient preemption provision will result in uneven privacy protection and thereby inhibit if not prevent the universal implementation of electronic data interchange for health care transactions.

We are also concerned that HR 4077 does not appear to apply to identifiable health care information in the non-treatment setting. In other words, information regarding health status in applications for life insurance and employment would not be protected and could be disclosed.

Our third principal concern is that the bill would not become effective until January 1, 1997, which could unduly delay the universal implementation of electronic data interchange in our health care system.

We also have an overriding concern regarding the possible complications and opportunity for game playing that may arise from the three trustee arrangement contemplated in the bill. In order to be enforceable, those regulated by the Act must know with reasonable certainty what regulations and requirements they must follow. Because, however, a given entity may at any time be a health use trustee, a public health trustee, and a special purpose trustee depending on the specific set of circumstances, it would be difficult if not impossible to assure that it was complying with the right set of rules. Furthermore, entities falling into more than one class of trustee would have to establish different sets of controls to protect privacy in different transactions.

We would, therefore, urge careful examination of the trustee concept to explore whether it could be simplified, and to carefully consider alternative solutions to the problem. Solutions might include establishment of only two trustee categories, for example, health use trustees, which should include employers and others maintaining health-related information in non-patient settings, and special purpose trustees, and exempting certain users from certain of the Act's requirements. For example, law enforcement agencies, as special use trustees, should not be required to permit access to or correction of records, or to provide a notice of information practices.

We also note that HR 4077 assigns to the Secretary of Health and Human Services the responsibility for administering and enforcing the Act. This, as we noted earlier, may be inappropriate in that the Department

WEDI TESTIMONY**Page 7**

of Health and Human Services (as are the Departments of Defense and Veterans Affairs) would be regulated under the Act. For that reason, we urge that consideration be given to assigning enforcement and administrative responsibility to an independent governmental agency that is neither a health care provider nor payer.

SUMMARY

In conclusion, WEDI believes that in order to make possible the many benefits of universal electronic data interchange in health care transactions, the health care industry, including private and public payers, providers and vendors of information services, must be able to travel the information superhighway without having to consider 51 different rules of the road for privacy protection.

WEDI also urges that privacy protection is warranted for identifiable health care information obtained in non-patient settings, and that the responsibility for administering and enforcing federal privacy legislation be assigned to an agency that is not itself a health care provider or payer. Furthermore, WEDI has recommended five principles for privacy protection that should be incorporated in security standards.

Finally, WEDI urges that the legislation be uncomplicated and enforceable, provide appropriate penalties for violation, and be implemented as soon as possible.

WEDI looks forward to working with your committee and with the Congress to develop meaningful and appropriate legislation that facilitates the universal implementation of electronic data interchange in health care while protecting the privacy rights of individuals.

Thank you for your attention. I'll be happy to answer any questions you may have.



Executive Summary

Workgroup for Electronic Data Interchange
October 1993

In November 1991, the Workgroup for Electronic Data Interchange (WEDI) was established in response to the challenge to reduce administrative costs in the nation's health care system. A voluntary, public-private task force, WEDI developed an action plan to streamline health care administration by standardizing electronic communications across the industry.

In July 1992, WEDI published a report that outlined the steps necessary to make electronic data interchange (EDI) routine for the health care industry by 1996 (refer to Addendum 1, "1992 WEDI Recommendations"). The Workgroup envisioned a health care industry transacting business electronically, using one set of electronic standards and interconnecting networks. Since that publication, the health care industry independently pushed forward and made substantial gains with EDI implementation:

- ◆ ASC X12 [an accredited American National Standards Institute (ANSI) Committee] approved the claim and eligibility standards for trial use.
- ◆ The Insurance Subcommittee of ASC X12 formed new workgroups to develop other standards required by the health care industry.
- ◆ HCFA initiated the use of Health Care Claim and Health Care Claim Payment/Advice standards and developed EDI implementation guides for Medicare Part A Intermediaries and Part B Carriers consistent with the ASC X12 standards.

- ◆ The private sector began developing EDI implementation guides.
- ◆ Efforts toward standardizing data content increased.
- ◆ EDI awareness and participation heightened.

WEDI reconvened in 1993 to resolve remaining implementation obstacles and to:

- ◆ Strengthen the understanding of and commitment to EDI among the health care industry, policymakers, and consumers by: developing a targeted plan for using industry resources to educate key audiences on EDI, encouraging participation in demonstration projects that prove EDI benefits and cost savings, and expanding membership to reflect more broadly the key constituencies affected by EDI.
- ◆ Work for enactment of preemptive federal confidentiality protection for individually identifiable health care information in an electronic environment.
- ◆ Develop a strategy to facilitate quick, industry-wide transition to EDI, including universal identifiers for patients, providers, and payors; health identification cards; coordination of benefits in electronic environments; and implementation guidance for data standards.
- ◆ Work with appropriate parties to ensure the health care industry can meet WEDI's target of universal adherence to uniform data content by 1996.
- ◆ Provide additional data to the industry on the cost benefits of EDI, using WEDI demonstration projects as a primary source (refer to Addendum 2, "1992 Findings" and Appendix 7, "Short-Term Strategies").
- ◆ Monitor the industry's progress toward the use of data standards and EDI.
- ◆ Provide basic telecommunications requirements and promote WEDI's goal of clearinghouse accreditation by 1994.
- ◆ Serve as a resource to work cooperatively with the National Association of Insurance Commissioners and state governments to coordinate state and national efforts on administrative simplification.

WEDI expanded its financial analysis to encompass eleven health care transactions. Newly available data were added to estimate the potential savings for providers and to update the estimated savings for payors and employers. Additionally, the cost of implementing EDI was added to achieve a more comprehensive picture of EDI's financial impact on the health care industry.

WEDI's 1993 financial analysis concludes that combining the estimated implementation costs and the gross administrative savings potential, the cumulative net savings over the next six years (to the year 2000) is estimated to total over \$42 billion. Although the estimated net savings may not translate directly to hard dollar savings for the nation's health care system, EDI savings will allow health care enterprises to reallocate resources from administrative activities to enhance quality, patient care, and customer service.

To achieve this large cost savings, WEDI's eleven Technical Advisory Groups developed the following major recommendations. These recommendations, along with additional "key" supporting recommendations, are provided, in full, in the "Report" section of this publication. They are summarized below according to the Technical Advisory Group that developed the recommendation:

1. Require specific and defined instructions through implementation guides to support uniform data content and coding structures (*Standards Implementation and Uniform Data Content*).
2. Develop a network architecture to support a broad array of applications, communications, access methods, protocols, and line speeds (*Network Architecture and Accreditation*).
3. Enact the model federal preemptive legislation drafted by WEDI to preserve confidentiality and privacy rights of individually identifiable health care information (*Confidentiality and Legal Issues*).
4. Identify unique, standard identification numbers to promote industry standardization and uniformity of health care data (*Unique Identifiers for the Health Care Industry*).
5. Develop and promote a comprehensive education and publicity work plan designed to provide standardized, economically affordable and geographically accessible education opportunities for all EDI constituents (*Education and Publicity*).
6. Develop an ASC X12 standard for data content and format for health identification cards (*Health Identification Cards*).
7. Continue demonstration projects that are ecumenical, identifiable to the public, demonstrate industry cooperation, leverage existing infrastructures, add something new, measure results, and meet aggressive time frames to demonstrate that technology is currently available to implement WEDI recommendations (*Short-Term Strategies*).

8. Clearly delineate state and federal roles for EDI implementation (*State/Federal Role*).
9. Provide ongoing analysis of the financial implications of EDI implementation (*Financial Implications*).
10. Automate the Coordination of Benefits process (*Coordination of Benefits*).
11. Use electronic environments and standardized data to improve fraud detection (*Health Care Fraud Prevention and Detection*).

These recommendations represent the consensus of the Steering Committee but do not necessarily represent the policy of any particular member organization participating in the WEDI process.

Significant progress has been made over the last year in the development of ASC X12 standards, increased volume of business conducted electronically, and new awareness and acceptance of WEDI's vision. However, much still remains to be accomplished. WEDI is committed to the aggressive goals outlined in the 1993 *WEDI Report* and to working in partnership with the Administration on Health Care Reform.

WEDI applauds recognition, by the Administration and a growing number of members of Congress, of the critical role that EDI must play in the nation's health care system. Many of their proposals build on WEDI's work and recommendations.



Appendix 3

Confidentiality and Legal Issues

Technical Advisory Group White Paper
October 1993

Introduction	3-3
Recommendation and Charge From the 1992 WEDI Report	3-3
Summary of "Health Information Confidentiality and Privacy Act of 1993"	3-4
Antitrust Review	3-12
Technical Advisory Group	3-13
Addenda	
Addendum 1: Text of Proposed "Health Information Confidentiality and Privacy Act of 1993"	3-15

Introduction

This White Paper responds to Recommendation Number 8 in the 1992 *WEDI Report* to the Secretary of the Department of Health and Human Services (HHS). The White Paper offers, for consideration by the Administration and Congress, a proposed federal bill designed to facilitate achieving the goal of reducing total administrative costs associated with health care claims processing and payment, including appropriate utilization review, through the use of electronic data interchange between providers and third party payors, while observing applicable requirements regarding confidentiality of health care information.

This paper summarizes the proposed bill, noting the Confidentiality and Legal Issues Technical Advisory Group's (TAG) intent, where appropriate, in order to provide a "legislative history" that will facilitate its interpretation and foster a common understanding of its provisions.

Recommendation and Charge from the 1992 WEDI Report

Recommendation Number 8 in the 1992 *WEDI Report* urged Congress to enact preemptive legislation governing confidentiality by the 4th Qtr '93 "to facilitate and ensure the uniform, confidential treatment of identifiable information in electronic environments."

The recommendation noted that WEDI would create a task force to coordinate with other relevant groups, and to assist in the timely technical drafting of this legislation, which should:

- ◆ Establish uniform requirements for the preservation of confidentiality and privacy rights in electronic health care claims processing and payment;
- ◆ Address the collection, storage, handling and transmission of individually identifiable health care data, including initial and subsequent disclosures, in electronic transactions by all public and private payors, providers of health care, and all other entities involved in the transactions;
- ◆ Exempt state public health reporting laws;

- ◆ Delineate protocols for secure electronic storage and transmission of health care data;
- ◆ Specify fair information practices that ensure a proper balance between required disclosures, use of data, and patient privacy;
- ◆ Require publication of the existence of health care data banks;
- ◆ Encourage use of alternate dispute resolution mechanisms, where appropriate;
- ◆ Establish that compliance with the Act's requirements would serve as a defense to legal actions, based on charges of improper disclosure;
- ◆ Impose penalties for violation of the Act, including civil damages, equitable remedies, and attorney's fees, where appropriate; and
- ◆ Provide enforcement by government officials and private, aggrieved parties.

Summary of "Health Information Confidentiality and Privacy Act of 1993"

As indicated in the preamble, the Act is designed to:

- ◆ Preserve confidentiality and privacy rights in individually identifiable health care information that is collected, stored, processed, or transmitted in electronic form;
- ◆ Preempt state laws that relate thereto, except public health reporting laws;
- ◆ Establish a mechanism for promulgating regulations that delineate protocols for securing such information when collected, stored, processed or transmitted in electronic form, and that set forth fair information practices;
- ◆ Require publication of the existence of health care data banks;
- ◆ Encourage the use of alternative dispute resolution mechanisms to resolve certain disputes under the Act; and
- ◆ Establish penalties for violating the Act.

To these ends, the Confidentiality and Legal Issues TAG intends that the Act be construed so as to broadly protect individually identifiable health care information from improper and unauthorized disclosures in an electronic environment, while facilitating the prompt and universal implementation of electronic data interchange for legitimate and necessary health care transactions.

The Act is not intended to relate to the privacy and confidentiality of identifiable health care provider information as it was considered beyond the scope of the TAG's charge.

Scope (Section 2)

In order to afford appropriate protection from unauthorized disclosures of individually identifiable health care information, the Act's requirements are intended to apply to all entities, including public and private third party payors and providers, that collect, store, process, or transmit such information in electronic form. The Act protects individually identifiable health care information, as defined in Section 3, but does not affect federal and state laws that require reporting of identifiable information to public health authorities (i.e., laws that require reporting of sexually transmitted diseases).

The TAG believes that applying the Act to non-electronic media may be counter-productive to WEDI's goal to use EDI universally for key health care transactions. The Act fulfills the TAG's charge and accomplishes WEDI's objective by facilitating and ensuring the uniform, confidential treatment of identifiable health care information in electronic environments. Because uniform requirements for privacy protection in health care transactions are important to providers, payors, vendors, and consumers, establishing a uniform regulatory environment for health care information in a form that is *not* electronic could remove an important incentive for migrating to EDI.

Definitions (Section 3)

The TAG has not designated the Secretary who will promulgate regulations and administer the Act. Although the Secretary of the Department of Health and Human Services may be the logical choice, concerns were expressed over the fact that HHS would be subject to the Act's requirements as an entity that collects, stores, processes, and transmits health care information in electronic form, and that the dual roles of the regulator and the regulated would appear to be a conflict of interest. Accordingly, the TAG recommends that responsibility for implementing the Act be

assigned either to an existing or new administrative officer or agency not otherwise responsible for administering or providing health care programs.

The Act defines "disclosure" to include "redisclosure," and the TAG intends the provisions regarding disclosure to be strictly construed as to afford maximum protection to the individual.

The TAG intends that the remaining definitions be construed as to broadly apply the Act's protections.

Preemption (Section 4)

The 1992 *WEDI Report* noted that "existing laws and regulations present a barrier to promoting electronic data interchange (EDI) in the health care marketplace," and that "current state laws may not recognize the transfer of key information in electronic form, or may prohibit the exchange of claim payment data without the written consent of the patient." The Report recognized that the many state and federal laws and regulations defining obligations regarding confidentiality of health care data require that payors and providers research each state's law in order to ensure compliance with the variety of potentially conflicting rules. WEDI found this not in the best interests of patients, providers, or payors because it is burdensome and costly, and creates a system where confidentiality rights vary widely from state-to-state.

In order to effectively, efficiently, and promptly achieve the objectives of facilitating the use of electronic data interchange in health care while affording appropriate and universal privacy and confidentiality protections, the TAG intends that federal law occupy the field and completely preempt the application of state law to the collection, storage, processing, and transmission of individually identifiable health care information in electronic form. Thus, the Act preempts state "quill pen" laws (laws requiring that certain medical records be in writing) and other state laws to the extent that they relate to matters regulated under the Act. However, in order to ensure that there are no gaps in protection, the federal preemption does not take effect until regulations implementing the Act are effective.

Standards for Information Practices (Section 5)

The Act requires the Secretary to promulgate regulations that establish appropriate levels of security, standards, and controls to ensure privacy and confidentiality, while considering the nature of the information and the relative risks of disclosure.

Accordingly, the security, standards and control levels established by the Secretary should vary with the nature of the information, the degree of risk to the individual, and the particular functions being performed by the entities involved.

The Act sets forth five principles to be incorporated in the regulations:

1. Guarantee the individual's right to know that identifiable health care information is collected, stored, or processed, and for what purpose it is used;
2. Assure that the information is collected, processed, stored, and transmitted only as required for a legitimate purpose;
3. Require that persons collecting information notify individuals of their rights under the Act;
4. Guarantee an individual's right of access to information from the person collecting the information; and
5. Require persons collecting, processing, storing, or transmitting identifiable information to implement the standards and controls promulgated by the Secretary.

To ensure that individuals are efficiently informed of their rights under the Act (while minimizing the amount of paper), the Act requires only that the entity collecting identifiable health care information from the individual provide the required statement, which must be in a form prescribed by the Secretary. The TAG intends that the prescribed form and the information provided the individual be easy to read and understandable, with codified values explained, and where appropriate, bilingual.

Disclosure (Section 6)

Generally, the Act requires that disclosures of individually identifiable health care information be authorized, and that persons collecting or storing the

information maintain a record of all external disclosures. The TAG strongly recommends that no exceptions be made for the record-keeping requirement for those entities making external disclosures of individually identifiable health care information. The TAG recognizes that added costs and burdens may be associated with maintaining such a record. There was an overriding sentiment, however, in favor of an individual's right to know, and the opportunity to make any necessary corrections outweighed the added burden of maintaining a record of all external disclosures.

Disclosures without authorization are permitted, however, in certain, specified circumstances. For example, disclosures to agents and employees obligated to maintain confidentiality are permitted to the extent necessary to enable the disclosing person to carry out lawful activities, as are certain disclosures to government authorities, disclosures to a successor in interest, disclosures for qualified research projects, disclosures by family members (unless expressly limited or prohibited), and disclosures pursuant to compulsory process or court order.

Publication (Section 7)

The Act requires that, pursuant to regulations, persons collecting identifiable health care information periodically publicize its existence and provide information regarding procedures for obtaining and correcting the information.

The TAG intends that the requirement of publication apply only to persons collecting the information from the individual, and *not* to those merely storing, processing, or transmitting the information. Accordingly, the individual's initial request to obtain or correct the information would normally be directed to the collector, who would then be responsible for forwarding the request to those entities that stored or processed the information, as shown on the record of disclosures that are maintained as required by persons collecting or storing information under Section 6.

In formulating the publication requirement, the TAG was mindful of the potential cost and administrative burdens that might be placed on persons collecting identifiable health care information (including employers, providers, and third party payors), and to the possibility that it might give rise to an increased number of requests for health records. Accordingly, the TAG intends that the publication requirement be detailed in regulations and developed with significant contributions from all interested and affected parties, as required by Section 10 of the Act. It will also take into account the cost and other concerns, and not unduly burden collectors of identifiable health care information. Such regulations could,

for example, specify the language for the disclosure, and set forth acceptable means such as brochures, signs, statements in bills, and explanations of benefits.

Furthermore, Section 8 of the Act, which provides detailed procedures for amending individually identifiable health care information, contains sufficient safeguards, including the requirement that amendment requests be in writing, to deter abuse of the right to amend. In any case, the TAG believes that the publication requirement is necessary and appropriate to provide individuals with sufficient information to permit them to exercise their rights under the Act.

Amendment of Individually Identifiable Health Care Information (Section 8)

This Section specifies the procedures for requesting amendment of individually identifiable health care information, and outlines the requirements necessary for responding to and handling requests for persons collecting, storing or processing such information. If the amendment is not made within 30 business days from receipt of the request, the person possessing the information must so notify the individual, indicating the reasons for refusal and the right to file a statement of correction, which must be included in any subsequent disclosure. If the amendment is made, notices must be sent to specified persons who had provided or received the information that has been amended.

The detailed procedures are intended to provide an orderly method for assuring the accuracy of identifiable health care information. The TAG believes that the Act establishes an appropriate balance between the rights of individuals and the obligations of entities possessing the information.

Alternative Dispute Resolution (Section 9)

Responding to WEDI's July 1992 recommendation that alternative dispute resolution mechanisms be encouraged, the Act requires the Secretary to promulgate regulations promoting, but not necessarily requiring, resolution of disputes arising under the Act through such mechanisms.

Promulgation of Regulations (Section 10)

The Act requires the Secretary to follow the procedures specified in the Negotiated Rulemaking Act of 1990 in promulgating regulations. That Act is permissive, however, in that it allows an administrative agency to establish a negotiated rulemaking committee to develop a proposed regulation if the agency head determines that use of the procedure is in the public interest. If the decision to establish a rulemaking committee is made, notice must be published in the Federal Register indicating the intention to establish the committee; the description of the subject and scope of the rule to be developed; a list of interests likely to be significantly affected; a list of persons to represent these interests and the agency on the committee; a proposed agenda and schedule; a solicitation for comments on the proposal to establish the committee and its proposed membership; and an explanation of how to apply for or nominate a person for committee membership.

The agency must consider the comments. If a committee is formed, it must attempt to reach a consensus on a proposed rule. No further responsibilities are assigned to the committee, and the agency is not required to adopt the committee's recommendations.

The proposed Act provides, however, that if a negotiated rulemaking committee is not named, the Secretary shall nevertheless appoint and consult with an advisory group of between seven and twelve individuals representing specified areas, including providers, payors, administrators, and consumers of health care. The TAG believes that the complex and rapid technological advancements characteristic of electronic data interchange, in addition to the serious issues surrounding the need to protect the privacy and confidentiality of individually identifiable health care information (in electronic form, in particular), dictates the need for reliance on such an advisory group in developing regulations for implementing the Act.

Civil Remedies (Section 11)

The Act affords aggrieved individuals a private right of action for civil relief, and grants exclusive jurisdiction to United States District Courts. In addition to injunctive relief, the individual may recover actual damages, attorneys' fees and other costs, and, if the violation resulted from willful or grossly negligent conduct, up to \$10,000 exclusive of actual loss.

Civil Money Penalties (Section 12)

The Act also subjects persons who knowingly disclose information in violation of the Act to civil monetary penalties as specified for single and multiple violations, and to a money penalty of up to \$100,000 if the Secretary finds that the violations constitute a general business practice.

The TAG believes that penalties for violations must be sufficient in order to foster compliance, yet not so high as to inhibit their imposition. The penalties suggested should achieve the necessary balance.

Immunity (Section 13)

The Act specifies that if an allegedly improper disclosure was made in accordance with the requirements of the Act and regulations, it constitutes an affirmative defense.

The TAG intends that persons able to show compliance with the security and other requirements specified in the Act and regulations have an affirmative defense to actions charging improper disclosure.

Criminal Penalties for Obtaining Individually Identifiable Health Care Information Through False Pretenses or Theft (Section 14)

The Act establishes criminal penalties (fines of up to \$50,000, or up to six months imprisonment, or both, for each offense) for persons requesting or obtaining individually identifiable health care information under false or fraudulent pretenses. In addition, persons who request or obtain such information under false or fraudulent pretenses, or who unlawfully take such information and who intentionally use, sell or transfer it for profit, may be fined up to \$100,000 or imprisoned for up to two years, or both, for each offense.

The TAG believes that meaningful criminal penalties are necessary to discourage persons from stealing or fraudulently requesting or obtaining information protected by the Act.

Severability (Section 15)

This Section provides that if any portion of the Act is held invalid, it shall not affect any other provisions that can be given effect without the invalid provision.

Effective Date (Section 16)

With the exception of Section 4, which delays the preemption of state laws until regulations implementing the Act are effective, the Act shall become effective upon enactment.

Antitrust Review

As part of its charge, counsel reviewed the white papers prepared by each of the Technical Advisory Groups to monitor compliance with applicable antitrust principles. In addition, counsel addressed Technical Advisory Group members regarding antitrust compliance issues at their February 22, 1993 meeting, and copies of the Antitrust Compliance Guide for the WEDI project were distributed to the Chairs of each Technical Advisory Group in March 1993 for review with members.

Technical Advisory Group

Co-Chairs

Marjorie Carey, Esq.
American Hospital Association

Joel E. Gimpel, Esq.
Blue Cross and Blue Shield Association

Members

Bente E. Cooney
National Committee to Preserve
Social Security and Medicare

Russ Fairbanks, Esq.
Electronic Data Systems

Jerry Kurtvka
Bank One

Hilary Lewis, Esq.
American Medical Association

Jim Orr
Blue Cross of California

Hank Palacios
Bureau of Census

Tim Ryan, Esq.
The Travelers Insurance Company

Michelle Thorne, Esq.
American Dental Association

Addenda

Addendum 1: Text of Proposed "Health Information Confidentiality and Privacy Act of 1993"

MODEL FEDERAL LEGISLATION

CONFIDENTIALITY OF ELECTRONIC HEALTH CARE INFORMATION

A BILL

To provide for the preservation of confidentiality and privacy rights in the collection, storage, processing and transmission of individually identifiable health care information (including initial and subsequent disclosure) in electronic form; to preempt state laws relating thereto, except public health reporting laws; to establish a regulatory mechanism for delineating protocols for securing electronic collection, storage, processing, and transmission of such health care information, and for fair information practices; to require publication of the existence of health care data banks; to encourage the use of alternative dispute resolution mechanisms, where appropriate, for resolving disputes arising under this Act; and to establish penalties for violation.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1 - SHORT TITLE

This Act may be cited as the "Health Information Confidentiality and Privacy Act of 1993."

SECTION 2 - SCOPE

- A. Applicability. This Act shall apply to the collection, storage, processing, and transmission of individually identifiable health care information (including initial and subsequent disclosures) in electronic form by all persons, including but not limited to public and private third-party payors and providers of health care.

- B. **Protection.** The protections of this Act shall extend to individuals who are the subject of individually identifiable health care information that is collected, stored, processed or transmitted in electronic form.
- C. **Exemptions.** This Act shall not apply to federal or state laws or regulations that require reporting of individually identifiable health care information to public health authorities.

SECTION 3 - DEFINITIONS

For purposes of this Act:

- A. **"Disclosure"** includes the initial release and any subsequent redisclosures of individually identifiable health care information.
- B. **"Electronic form"** means all mechanical, non-paper formats, including fiberoptic transmission and laser disc storage.
- C. **"External Disclosure(s)"** means:
 - (1) All disclosures of individually identifiable health care information to person(s) who are not employed or credentialed by, or who do not have an independent contractor relationship with a payor or provider; and
 - (2) Which are made on behalf of the individual and are directly related to either the adjudication of a claim, coordination of benefits, or to the medical treatment of an individual.
- D. **"Health care"** means:
 - (1) Any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service or procedure provided by a provider:
 - (a) with respect to an individual's physical or mental condition; or
 - (b) affecting the structure or function of the human body or any part thereof, including, but not limited to, banking of blood, sperm, organs, or any other tissue; and
 - (2) The prescription, sale or dispensing of any drug, substance, device, equipment, or other item to an individual or for an individual's use for health care.

- E. "Individual" means a natural person who is the subject of individually identifiable health care information, and includes the individual's legal representative.
- F. "Individually identifiable health care information" means any data or information that identifies or can reasonably be associated with the identity of an individual, either directly or by reference to other publicly available information, and:
 - (1) Relates to the individual's health history, health status, health benefits, or application therefor; or
 - (2) Is obtained in the course of an individual's health care from a provider, from the individual, from a member of the individual's family, or from a person with whom the individual has a close personal relationship.
- G. "Person" means a government, governmental subdivision, agency or authority, natural person, corporation, estate, trust, partnership, association, joint venture, and any other legal entity.
- H. "Provider" means a person that is duly authorized, or that represents itself as being duly authorized to provide health care.
- I. "Secretary" means . . .

SECTION 4 - PREEMPTION

Unless otherwise provided in Section 2 C, upon the effective date of regulations implementing this Act, no effect shall be given to any provision of state law that requires individually identifiable health care information to be maintained exclusively in written rather than electronic form or to any provision of state law to the extent it relates to the matters covered in this Act, including the preservation of confidentiality and privacy rights in the collection, storage, processing, and transmission of individually identifiable health care information (including initial and subsequent disclosures) in electronic form by all involved in such transactions.

SECTION 5 - STANDARDS FOR INFORMATION PRACTICES

- A. The Secretary shall, by regulation, establish appropriate levels of security, standards, and controls including but not limited to passwords, access codes, restrictions on access, limitations on networking and electronic data sharing, and protocols and procedures for preventing computer sabotage, for collecting, storing, processing and transmitting individually identifiable health care information in electronic form so as to ensure the

privacy and confidentiality of such information, taking into consideration the nature of the information and relative risks of disclosure.

- B. The regulations promulgated pursuant to Section 5 A shall incorporate the following principles:
- (1) The individual shall have the right to know that individually identifiable health care information concerning the individual is collected, stored, processed or transmitted by any person, and to know for what purpose such information is used.
 - (2) Individually identifiable health care information shall be collected, processed, stored and transmitted only to the extent necessary to carry out a legitimate purpose for which the individual has granted consent.
 - (3) Each person collecting individually identifiable health care information from an individual shall notify the individual of his or her right to receive a statement, in the style and form prescribed by the Secretary, summarizing the individual's rights pursuant to this Act.
 - (4) The individual shall have a right of access to individually identifiable health care information concerning the individual from the person collecting such information, the right to have a copy of such information after payment of a reasonable charge, and the right to have a notation made with or in such information of any amendment or correction requested by the individual.
 - (5) Persons collecting, processing, storing or transmitting individually identifiable health care information shall implement or cause to be implemented as the case may be, the appropriate security standards and controls promulgated by the Secretary to assure the accuracy, reliability, relevance, completeness, timeliness and security of such information.

SECTION 6 - DISCLOSURE

- A. Disclosure. Except as authorized in Section 6 D, no person other than an individual shall disclose individually identifiable health care information to any other person without the individual's valid authorization as provided in Section 6 C. No person shall disclose such information except in accordance with the terms of such authorization, unless otherwise authorized under Section 6 D.

- B. Record of Disclosures. Each person collecting or storing individually identifiable health care information shall maintain a record of all external disclosures made on behalf of a provider, payor or individual, of such information.
- C. Individual Authorization: Requirements for Validity.
- (1) To be valid, an authorization to disclose individually identifiable health care information must –
 - (a) Identify the individual;
 - (b) Describe the health care information to be disclosed;
 - (c) Identify the person to whom the information is to be disclosed;
 - (d) Describe the purpose of the disclosure;
 - (e) Indicate the length of time for which the individual's authorization will remain valid;
 - (f) Be either,
 - (i) In writing, dated and signed by the individual; or
 - (ii) In electronic form, dated and authenticated by the individual using a unique identifier; and
 - (g) Not have been revoked under Section 6 C (2).
 - (2) Revocation of Individual's Authorization. An individual may revoke the individual's authorization at any time, unless disclosure is required to effectuate payment for health care that has been provided to the individual, or other action has been taken in reliance on the individual's authorization. An individual may not maintain an action against a person for disclosure of individually identifiable health care information made in good faith reliance on the individual's authorization, provided the disclosing person had no notice of the revocation of the individual's authorization at the time disclosure was made.
 - (3) Record of Individual's Authorizations and Revocations. Each person collecting or storing individually identifiable health care information shall maintain a record of each individual's authorization and revocation thereof, and such record shall become part of the

individually identifiable health care information concerning such individual.

- (4) No Waiver. Except as provided by this Act, an authorization to disclose individually identifiable health care information by an individual is not a waiver of any rights an individual has under other federal or state statutes, the rules of evidence, or common law.
- D. Disclosure Without An Individual's Authorization. A person may disclose individually identifiable health care information without the individual's authorization required in Section C if:
- (1) The disclosure is by a family member or by any other person with whom the individual has a close personal relationship, unless such disclosure is expressly limited or prohibited by the individual;
 - (2) The disclosure is only to the extent necessary for the disclosing person to carry out its lawful activities and is to the disclosing person's agent, employee, or independent contractor who is under an obligation to hold the individually identifiable health care information in confidence and not to use such information for any purpose other than the lawful purpose for which the information was obtained by the disclosing person;
 - (3) The disclosure is to a provider who is providing health care to the individual except as such disclosure is limited or prohibited by the individual;
 - (4) The disclosing person reasonably believes that disclosure is necessary to avoid or minimize imminent danger to the health or safety of any individual, but only to the extent necessary to avoid or minimize such danger or emergency;
 - (5) The disclosure is to a member of the individual's immediate family, or to any other individual with whom the patient is known to have a close personal relationship, if such disclosure is made in accordance with good medical or other professional practice, unless such disclosure is expressly limited or prohibited by the individual;
 - (6) The disclosure is to a successor in interest to the person maintaining the individually identifiable health care information, provided, however, that no person other than a provider or the estate of a deceased provider shall be considered a successor in interest to a provider;

- (7) The disclosure is to federal, state, or local government authorities, to the extent the person holding the individually identifiable health care information is required by law to report specific individually identifiable health care information:
 - (a) when needed to determine compliance with state or federal licensure, certification, or registration rules or laws; or
 - (b) when needed to protect the public health;
- (8) The disclosure is to a person solely for purposes of conducting an audit, if that person agrees in writing:
 - (a) to remove or destroy, at the earliest opportunity consistent with the purpose of the audit, information that would enable identification of the individual;
 - (b) not to disclose in any report any individually identifiable health care information; and
 - (c) not to further disclose the information, except to accomplish the audit or to report unlawful or improper conduct involving health care fraud by a provider or the individual or other unlawful conduct by a provider;
- (9) The disclosure is for use in a research project that:
 - (a) is of sufficient importance to outweigh any potential harm to the individual that would result from the disclosure;
 - (b) is reasonably impracticable without the use of the individually identifiable health care information;
 - (c) contains reasonable safeguards to protect the information from redisclosure;
 - (d) contains reasonable safeguards to protect against identifying, directly or indirectly, any individual in any report of the research project;
 - (e) contains procedures to remove or destroy at the earliest opportunity, consistent with the purposes of the project, information that would enable identification of the individual, unless retention of identifying information is required for purposes of another research project that also satisfies the requirements of this Section; and

- (f) the person agrees in writing:
 - (i) to remove or destroy, at the earliest opportunity consistent with the purpose of the research information that would enable identification of the individual;
 - (ii) to not disclose individually identifiable health care information, except as necessary to conduct the research project;
- (10) The disclosure is in accordance with a discovery request:
 - (a) Before service of a discovery request on a person maintaining individually identifiable health care information, an attorney shall provide advance notice to the person and to the individual involved or the individual's representative or attorney through service of process or first class mail, indicating what information is sought, and the date by which a protective order must be obtained to prevent the person from complying. Such date shall give the individual and the person adequate time to seek a protective order, but in no event be less than fourteen days after the date of service of such notice;
 - (b) Without the individual's authorization, a person may not disclose the information sought under paragraph (a) if the requestor has not complied with the requirements of paragraph (a). In the absence of a protective order issued by a court of competent jurisdiction forbidding compliance, the person shall disclose the information in accordance with this section. In the case of compliance, the request for discovery or compulsory process shall be maintained by the holder thereof with the individual's health care information;
 - (c) Production of individually identifiable health care information under this section, in and of itself, does not constitute a waiver of any privilege, objection, or defense existing under other law or rule of evidence or procedure;
- (11) The disclosure is to federal, state or local law enforcement authorities to the extent required or permitted by law;
- (12) The disclosure is directed by a court in connection with a court-ordered examination of an individual; or

(13) The disclosure is based on reasonable grounds to believe that the information is needed to assist in the identification of a deceased individual.

E. Obligations of Legal Representatives.

(1) A person authorized to act as an individual's legal representative may exercise the rights of the individual under this Act to the extent necessary to effectuate the terms or purposes of the grant of authority; but an individual who is a minor and who is authorized to consent to health care without the consent of a parent or legal guardian under State law may exclusively exercise the rights of an individual under this Act as to information pertaining to health care to which the minor lawfully consented.

(2) An individual's legal representative shall act in good faith to represent the best interests of the individual with respect to individually identifiable health care information.

SECTION 7 - PUBLICATION

Persons collecting individually identifiable health care information shall, pursuant to regulations, periodically publicize the existence of the information and provide information regarding procedures for obtaining and correcting the information.

SECTION 8 - AMENDMENT OF INDIVIDUALLY IDENTIFIABLE HEALTH CARE INFORMATION

A. Within thirty (30) business days from the date of receipt of a written request from an individual to amend any individually identifiable health care information about the individual within its possession, a person collecting, storing or processing such information shall either:

(1) Amend the portion of the recorded individually identifiable health care information identified by the individual, or

(2) Notify the individual of:

(a) Its refusal to make such, amendment;

(b) The reasons for the refusal, and

- (c) The individual's right to file a statement as provided in Subsection 8C.
- B. If the person amends information in accordance with Subsection 8 A above, the person shall provide the amendment to:
- (1) The individual;
 - (2) Any person specifically designated by the individual who may have, within the preceding two (2) years, received such information;
 - (3) Other persons who have systematically been provided such information within the preceding seven (7) years; provided, however, that the amendment or fact of deletion need not be furnished if the other person no longer maintains such information about the individual; and
 - (4) Any person that provided the information that has been amended.
- C. Whenever an individual disagrees with a person's refusal to amend individually identifiable health care information, the individual shall be permitted to file with such person:
- (1) A concise statement setting forth what the individual believes to be correct, relevant or fair information; and
 - (2) A concise statement of the reasons why the individual disagrees with the refusal to amend such information.
- D. If an individual files either statement as described in Subsection C above, the person shall:
- (1) Include the statement with the disputed individually identifiable health care information and provide a means by which anyone reviewing such information will be made aware of the individual's statement and have access to it;
 - (2) With any subsequent disclosure of the information that is the subject of disagreement, clearly identify the matter or matters in dispute and provide the individual's statement along with the information being disclosed; and
 - (3) Provide the statement to the persons and in the manner specified in Subsection 8 B above.

- E. The rights granted in this section shall not apply to individually identifiable health care information that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving the individual.

SECTION 9 - ALTERNATIVE DISPUTE RESOLUTION

The Secretary shall promulgate regulations that will promote the resolution of disputes arising under this Act through alternative dispute resolution mechanisms.

SECTION 10 - PROMULGATION OF REGULATIONS

- A. In promulgating regulations under this Act, the Secretary shall follow the procedures authorized under the "Negotiated Rulemaking Act of 1990," 5 U.S.C. §§ 581-590.
- B. If the Secretary determines that a negotiated rulemaking committee shall not be established as permitted by 5 U.S.C. § 583, the Secretary shall appoint and consult with an advisory group of knowledgeable individuals. The advisory group shall consist of at least seven (7) but no more than twelve (12) individuals from the following areas: (1) health care financing and reimbursement; (2) health care delivery, including representatives of health care professionals and health care entities; (3) third party payors/administrators, network administrators; and (4) health care consumers.
- C. The advisory group shall review all proposed rules and regulations and submit recommendations to the Secretary. The advisory group shall also assist the Secretary: (1) in establishing the standards for compliance with rules and regulations; and (2) in developing an annual report to the Congress on the status of the requirements set forth in this Act, their cost impact, and any recommendations for modifications in order to ensure efficient and confidential electronic data interchange of individually identifiable health care information.

SECTION 11 - CIVIL REMEDIES

- A. An individual aggrieved by a violation of this Act may maintain an action for relief as provided in this section.
- B. The district courts of the United States shall have exclusive jurisdiction in any action brought under the provisions of this section.

- C. The court may order a person maintaining individually identifiable health care information to comply with this Act and may order any other appropriate relief.
- D. If the court determines that there has been a violation of this Act, the aggrieved individual shall be entitled to recover damages for any losses sustained as a result of the violation; and, in addition, if the violation results from willful or grossly negligent conduct, the aggrieved individual may recover not in excess of \$10,000, exclusive of any loss.
- E. If an aggrieved individual prevails in an action brought under this section, the court, in addition to any other relief granted under this section, may award reasonable attorneys' fees and all other expenses incurred by the aggrieved individual in the litigation.
- F. Any action under this Act must be brought within two years from the date on which the alleged violation is discovered.

SECTION 12 - CIVIL MONEY PENALTIES

Any person that knowingly discloses health care information in violation of this Act shall be subject, in addition to any other penalties that may be prescribed by law --

- A. to a civil money penalty of not more than \$10,000 for each violation, but not to exceed \$50,000 in the aggregate for multiple violations; and, in addition -
- B. to a civil money penalty of not more than \$100,000 if the Secretary finds that violations of this Act have occurred with such frequency as to constitute a general business practice.

SECTION 13 - IMMUNITY

It shall be an affirmative defense in actions brought for improper disclosure of individually identifiable health care information that such disclosure was in accordance with the requirements of this Act and regulations promulgated pursuant to this Act.

SECTION 14 - CRIMINAL PENALTIES FOR OBTAINING INDIVIDUALLY IDENTIFIABLE HEALTH CARE INFORMATION THROUGH FALSE PRETENSES OR THEFT

- A. Any person who, under false or fraudulent pretenses, requests or obtains individually identifiable health care information shall be fined not more than \$50,000 or imprisoned not more than six months, or both, for each offense.
- B. Any person who unlawfully takes, or under false or fraudulent pretenses, requests or obtains individually identifiable health care information and who intentionally uses, sells or transfers such information for remuneration, for profit or for monetary gain shall be fined not more than \$100,000, or imprisoned for not more than two years, or both, for each offense.

SECTION 15 - SEVERABILITY

If any provision of this Act or its application to any person or circumstance is held invalid, it shall not affect other provisions or applications of this Act that can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

SECTION 16 - EFFECTIVE DATE

Except as provided in Section 4, this Act shall become effective upon enactment.

Mr. CONDIT. Ms. Frawley.

STATEMENT OF KATHLEEN FRAWLEY, DIRECTOR, WASHINGTON OFFICE, AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION

Ms. FRAWLEY. Thank you. Mr. Chairman and members of the subcommittee, my name is Kathleen A. Frawley, and I am director of the Washington, DC office for the American Health Information Management Association. AHIMA appreciates this opportunity to appear before the subcommittee to present its views on the Fair Health Information Practices Act of 1994.

The American Health Information Management Association represents 35,000 credentialed professionals responsible for managing the health care information that is an increasingly important component of our Nation's health care delivery system. AHIMA and its members support the need for Federal preemptive legislation that will establish uniform rules regarding the use and disclosure of identifiable health information.

In 1993, in order to address the need for Federal legislation, AHIMA drafted model language which has been shared with this subcommittee. We are pleased to see this bill incorporates many of the provisions of AHIMA's model language.

Mr. Chairman, AHIMA was deeply honored to be recognized by you in your remarks introducing H.R. 4077. During the past several months, there has been an emerging consensus regarding the need for Federal legislation.

The development of the national information infrastructure is a key component of health care reform. Efforts to reform this country's health care delivery system will rely heavily on administrative simplification and computerization of health information to control costs, improve quality of care, and increase efficiency. The increasing demand for data highlights the need for Federal preemptive legislation to protect the confidentiality of health information.

AHIMA believes that we cannot afford to wait to enact legislation. The Congress must act now and provide protections for health information. It is critical that any comprehensive health care reform proposal that passes the Congress contain specific provisions regarding privacy and confidentiality. It is noted that H.R. 4077 is expected to be offered as an amendment to the Health Security Act when the bill is marked up by the Committee on Government Operations. AHIMA strongly supports this initiative and is willing to assist if this course is taken.

AHIMA is pleased that H.R. 4077 contains many of the provisions based on a code of fair information practices that was contained in the AHIMA model language. We strongly support the concept that individuals have the right to know who maintains health information and for what purpose the information is used.

Section 111, inspection of protected health information, and section 112, amendment of protected health information, will provide all individuals the right to access their personal health information. Currently, this right does not exist in all 50 States.

AHIMA strongly supports the need for mechanisms that will allow individuals to enforce their rights. We are pleased to note that subtitle E addresses civil remedies, criminal penalties and al-

ternative dispute resolution. It should be noted, however, that the bill as currently drafted provides confidentiality obligations only with respect to protected health information.

It is our understanding that health information collected outside the treatment or payment process would not be covered. It is critical that the definition of protected health information be expanded to include all information related to an individual's health treatment.

While we agree that the concept of ownership of information is outdated, we are concerned that the bill's current approach to imposing rights and responsibilities based on certain classes of health information trustees does not reflect the reality of how patient records will increasingly be and are being created.

We would recommend that the bill be framed to protect all individually identifiable health information, regardless of the holder, rather than imposing obligations only on certain types of trustees.

We are unable to ascertain the effect of the preemption provisions in section 304. To the extent that States can impose more stringent requirements with respect to individually identifiable health information, any hope of administrative efficiency on a national scale will evaporate. We look forward to working with you on this issue.

There are some other issues that we believe must be addressed in this bill. In order to facilitate the development of computer-based patient records, State "quill pen" laws must be preempted. The Institute of Medicine report, "The Computer-Based Patient Record: An Essential Technology for Health Care," recommended the adoption of the computerized patient record by the year 2000, and the formation of a nationwide health information network.

However, as that report noted, there are States which require that medical records be written and signed. In order to facilitate the development of a national health information infrastructure, it is imperative that health information can be created, authenticated and retained in electronic form. We would recommend that the preemption section address this issue.

It is important to note that currently there are no Federal laws outlining timeframes for the retention of health information. Many States do have specific requirements. However, there is an absence of uniformity.

As the health care industry moves from paper to computer-based patient records, retention guidelines must be reexamined to support the development of longitudinal medical records on a national level.

Finally, there are vendors who provide data entry services for claims processing or transcription of medical reports who are currently using offshore personnel. It is important that these activities be reviewed to ensure they comply with section 152.

AHIMA commends you, Mr. Chairman, for introducing this very important piece of legislation. We would like to acknowledge the excellent work of your subcommittee staff, particularly Robert Gellman, chief counsel.

We look forward to working closely with the subcommittee in its ongoing efforts with this bill. Thank you.

[The prepared statement of Ms. Frawley follows:]

Mr. Chairman and Members of the Subcommittee:

My name is Kathleen A. Frawley, and I am Director of the Washington, D. C. Office for the American Health Information Management Association (AHIMA). AHIMA appreciates this opportunity to appear before the Subcommittee to present its views on the Fair Health Information Practices Act of 1994 (H. R. 4077).

The American Health Information Management Association (AHIMA) represents 35,000 credentialed professionals responsible for managing the health care information that is an increasingly important component of our nation's health care delivery system. AHIMA and its members support the need for federal pre-emptive legislation that will establish uniform rules regarding the use and disclosure of individually identifiable health information.

In 1993, in order to address the need for federal legislation, AHIMA drafted model language which has been shared with this Subcommittee. We are pleased to see that this bill incorporates many of the provisions of AHIMA's model language. Mr. Chairman, AHIMA was deeply honored to be recognized by you in your remarks introducing H. R. 4077.

NEED FOR FEDERAL LEGISLATION

During the past several months, there has been an emerging consensus regarding the need for federal legislation. The Office of Technology Assessment (OTA) report, Protecting Privacy in Computerized Medical Information, which was released at a hearing held by this Subcommittee last November, found that current laws, in general, do not provide consistent, comprehensive protection of health information confidentiality. Focusing on the impact of computer technology, the report concluded that computerization reduces some concerns about privacy of health information while increasing others. The report highlights the need for enactment of a comprehensive federal privacy law.

The public's concern about the confidentiality of health information was reflected in a poll conducted by Louis Harris and Associates for Equifax, Inc. The results of the Health Information Privacy Survey 1993 were released at a conference sponsored by AHIMA and Equifax in conjunction with the U. S. Office of Consumer Affairs on October 26, 1993. At this conference, Senator Patrick Leahy (D-VT) and Representative Pete Stark (D-CA) and several other panelists identified the need to address privacy of health information in any healthcare reform plan.

The survey found that a large majority of Americans (89%) believe reforming health care is one of the top domestic issues

facing the nation today. Fifty-six percent (56%) indicated strong support for comprehensive federal legislation to protect the privacy of medical records as part of healthcare reform.

There was high agreement on what should be included in national privacy legislation. Ninety-six percent (96%) believe federal legislation should designate all personal medical information as sensitive and impose severe penalties for unauthorized disclosure. Ninety-five percent (95%) favor legislation that addresses individuals' rights to access their medical records and creates procedures for updating or correcting those records.

The recently released Institute of Medicine report, Health Data in the Information Age: Use, Disclosure and Privacy, recommends that federal preemptive legislation be enacted to establish uniform requirements for the preservation of confidentiality and protection of privacy rights for health data about individuals.

HEALTH CARE REFORM AND THE NATIONAL INFORMATION INFRASTRUCTURE

The development of the national information infrastructure is a key component of healthcare reform. Efforts to reform this country's health care delivery system will rely heavily on administrative simplification and computerization of health information to control costs, improve quality of care and increase efficiency. The increasing demand for data highlights

the need for federal pre-emptive legislation to protect the confidentiality of health information.

In the Administration's Health Security Act (Title V, Subtitle B, Part 2), privacy of health information is addressed. Within two years of the enactment of this Act, the National Health Board would be responsible for the development of privacy and security standards to address unauthorized disclosure, and provide individuals with the right to access their personal health information. The Act requires that, within three years of enactment, the Board shall submit to the President and Congress a comprehensive legislative proposal, based on a Code of Fair Information Practices, to protect the privacy of individually identifiable health information.

AHIMA believes that we cannot afford to wait to enact legislation. The Congress must act now and provide protections for health information. It is critical that any comprehensive healthcare reform proposal that passes the Congress contain specific provisions regarding privacy and confidentiality. It is noted that H. R. 4077 is expected to be offered as an amendment to the Health Security Act (H. R. 3600) when the bill is marked up by the Committee on Government Operations. AHIMA strongly supports this initiative and is willing to assist if this course is taken.

AHIMA'S POSITION

AHIMA is pleased that H. R. 4077 contains many of the provisions based on a code of fair information practices that were contained in the AHIMA model language. We strongly support the concept that individuals have the right to know who maintains health information and for what purpose the information is used. Section 111, Inspection of Protected Health Information, and Section 112, Amendment of Protected Health Information will provide all individuals with the right to access their personal health information. Currently, this right does not exist in all fifty states.

Health information concerning an individual must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected. There must be limitations on the use and disclosure of individually identifiable health information. The bill does address these issues in Part 2, Use and Disclosure of Protected Health Information. Health information is used for a variety of legitimate purposes, including patient care, quality review, education, research, public health, and legal and financial interests. Regardless of the use or users, individuals must be assured that the information they share with healthcare professionals will remain confidential.

AHIMA strongly supports the need for mechanisms that will allow individuals to enforce their rights. We are pleased to note that Subtitle E addresses civil remedies, criminal penalties and alternative dispute resolution.

It should be noted, however, that the bill as currently drafted imposes confidentiality obligations only with respect to "protected health information". It is our understanding that health information collected outside the treatment or payment process would not be covered. It is critical that the definition of protected health information be expanded.

While we agree that the concept of ownership of information is outdated, we are concerned that the bill's current approach to imposing rights and responsibilities based on certain classes of health information trustees does not reflect the reality of how patient records will increasingly be and are being created. We would recommend that the bill be framed to protect all individually identifiable health information, regardless of the holder, rather than imposing obligations only on certain types of holders.

We are unable to ascertain the effect of the preemption provisions in Section 304. As the OTA report noted, our present system of protecting health information is based on a patchwork quilt of laws. To the extent that states can impose more stringent requirements with respect to individually identifiable

health information, any hope of administrative efficiency on a national scale will evaporate. We look forward to working with you on this issue.

There are some other issues that we believe must be addressed in this bill. In order to facilitate the development of computer-based patient records, state quill pen laws must be preempted. The IOM report, The Computer-Based Patient Record: An Essential Technology for Health Care, recommended the adoption of computer-based patient records by the year 2000 and the formation of a nationwide health information network. However, as that report noted, there are states which require that medical records be written and signed. In order to facilitate the development of a national health information infrastructure, it is imperative that health information can be created, authenticated and retained in electronic form. We would recommend that the preemption section address this issue.

It is important to note that, currently, there are no federal laws outlining time frames for the retention of health information. Many states do have specific requirements. However, there is an absence of uniformity. As the healthcare industry moves from paper to computer-based patient records, retention guidelines must be re-examined to support the development of longitudinal records on a national level.

Finally, there are vendors who provide data entry services for claims processing or transcription of medical reports who are

using offshore personnel. It is important that these activities be reviewed to ensure if they comply with Section 152.

CONCLUSION

AHIMA commends you, Mr. Chairman, for introducing this very important piece of legislation. We would like to acknowledge the excellent work of your Subcommittee staff, particularly Robert Gellman, Chief Counsel. We look forward to working closely with the Subcommittee in its ongoing efforts with this bill.

Thank you.

Mr. CONDIT. Thank you, Ms. Frawley.

Thank all of you for your participation this morning.

We have a few questions we'd like to ask.

I recognize that the bill, 4077, is not a perfect bill, and I'm committed to work with all of you to fix whatever problems we have.

Do any of you see any reason why we should not be able to reach an agreement on the fair information practices and pass this bill?

Dr. LEWERS. No, sir.

Mr. CONDIT. I guess the silence of everyone, you agree with that, that there should be no reason why we can't solve our problems?

Ms. FRAWLEY. Absolutely not, Mr. Chairman. I think that certainly the hearings that you held last November and certainly the hearings that have started, the number of reports that recently have come out from the Office of Technology Assessment and the recent Institute of Medicine report, clearly along with the Equifax-Harris survey, show there is tremendous support for Federal legislation.

I think all of us here agree that H.R. 4077 is a great first step and that, you know, there is an opportunity here to make sure that individually identifiable health information is protected.

Mr. CONDIT. One of my pet peeves since I have been here has been my concern about the cost of the legislation.

Can any of you identify any specific cost savings with uniformity? Will uniform Federal rules reduce the cost of transferring health data, especially in a computerized environment?

Mr. ENTIN. Well, I would certainly see that those kinds of savings are present if we go to a uniform system. If you look at networks, which is where we see the world going, networks of providers, networks in an area such as Washington, DC, will provide care to patients in at least three different jurisdictions. The elimination of the need to comply with three sets of laws pertaining to the maintenance and transmission of information, has to lead to the reduction of costs. So we think that it's an important contribution toward the overall problem of health restructuring.

Mr. GIMPEL. Mr. Chairman, also, the WEDI report identifies the possibility of reducing the costs of administering the health care system through the migration to electronic data interchange. To the extent that Federal legislation would facilitate that kind of migration, we would hope that costs of administering health care would be reduced or there would be some—at least, hassle factor, reducing—reduced as well.

Mr. CONDIT. Dr. Lewers.

Dr. LEWERS. Yes, we would agree with that, and in our written statement we have gone into some of these issues. I think we have to be very careful that we don't create issues in areas that we already have some protection and agencies that are working with this.

We have no problem with this going in with HHS. We would like to see that all of us are involved in the regulations as they are promulgated. And perhaps utilizing the negotiated rulemaking procedure would really assure some sort of factor that there is not the conflict of interest that was suggested in some of the testimony.

We think that let's not create a whole new bureaucracy to do this. Let's keep it similar, let's bring it out, let's keep the patient

uppermost in mind, and that confidentiality in mind, and we can do that without adding a great deal of cost.

Mr. CONDIT. Let me ask each of you, what is your single highest priority for changing the bill, and what is the worst mistake we have made so far? And I ask this in a constructive way, and I hope that you will answer in a constructive way.

Dr. LEWERS. We'll start off on the end of the table, I guess.

Our concern I think you have addressed, and that is the confidentiality issue and the protection of patient information. This is an area that we are concerned and that we would hold uppermost within the bill in all avenues as we look at it. I think the concern that I have heard and I have read is the issue of preemption and the State issues.

I'm from Maryland. Maryland has a very strong release bill that was passed 2 or 3 years ago. Most of the members that practice medicine don't know about that at this point in time. So patient education is an area that we see needs to be expanded, but we really have to preempt the State issues.

As stated, I work in an area where we deal with three States and so this gets very complicated. I think that's an area we'd like to see expanded as well.

Mr. CONDIT. Anybody else?

Mr. Entin.

Mr. ENTIN. I would agree. I think that preemption is the most important aspect to be addressed by the bill. Not only is it important that there be some form of uniformity across the country for purposes of ease of transmission, but even if we don't go to an electronic, automated approach, we have a patchwork of laws across the country that are not adequate in many States, in other States they are quite adequate.

I think that the issue of privacy is one that needs to be established at the Federal level in order to achieve the that kind of uniformity. I think that the other issue that we would urge the committee to consider is the trustee approach. We understand the concept and we understand that the intent behind it is to ensure that people in possession of information, are certainly aware of their obligations.

We think, however, that it is more complicated than it needs to be and that, in fact, it may reduce the ability of people to comply with the law because of the overcomplication of going to the three-trustee approach. We believe that you ought to follow the use of the information rather than the identity of the possessor of the information to achieve the same goals.

Mr. CONDIT. Mr. Gimpel.

Mr. GIMPEL. Yes, Mr. Chairman.

At the risk of echoing what my predecessors said, I would like to iterate those concerns. I think WEDI's first concern is the preemption issue, that we need "one rule of the road" rather than 51, and the simplification concern with the three-trustee arrangement.

I would also add that the use of the term "trustee" could bring some connotations that might be unintended, because the word "trustee" has some legal—brings along some legal baggage that perhaps is inappropriate for the legislation. So perhaps there ought

to be some definition of what that term means in the context of this legislation.

And the third piece is that we would have concern with assigning the oversight and administrative responsibility to an entity that is, in fact, one of the regulated entities under the act. There is a concern for a conflict of interest if HHS, which is both a provider and a payer of health benefits, is also the regulator.

Mr. CONDIT. Ms. Frawley.

Ms. FRAWLEY. I certainly concur with the other panelists on the issue of preemption and also again the concern that the trustee approach is somewhat complex and is difficult for individuals to understand what their rights and responsibilities are.

The other concern is just the definition of protected health information. We are concerned that it may be too narrow. It may not include information that is collected as the start of health screening process in conjunction with an application for insurance or conjunction with an application for employment.

And what we'd like to see is any individually identifiable health information, no matter where it originates, being protected by this bill. And I think that's an important issue.

Mr. CONDIT. Mr. Gimpel, I agree with the concern you raised about preemption, I think everybody has made reference to that. I look forward to working with everyone to try to find a solution.

You raise the issue of the use of health information in life insurance and employment. Does WEDI support a general Federal privacy law governing life insurance records, how about employment records?

Mr. GIMPEL. The WEDI version, the WEDI model, would apply to health care information in such settings as well as in the health care setting. So it does apply, those protections, to that information, yes.

Mr. CONDIT. So all the above?

Mr. GIMPEL. Yes.

Mr. CONDIT. Sort of complicates our task a little bit.

Mr. GIMPEL. It may complicate the task, but I believe that the feeling was is that why protect it in the health setting information if it can be disclosed by the employer who collects it in the employment application?

Mr. CONDIT. Ms. Frawley, is it fair to say that there is a lot of confusion and uncertainty on the part of medical professionals about the current rules for confidentiality of records? How many people really know the rules in their own State?

Ms. FRAWLEY. It's a very good point, Mr. Chairman. Right now individuals are continually struggling with the fact that we have multistate providers and payers, that requests for information may be received, and that many times individuals are not familiar with the current statutes and regulations in the State where the patient received care or the State where the payer may be located. And so certainly there is an absence of uniformity which is why we strongly support the need for the Federal legislation.

It's a very complex issue. Any medical record before it can be released, we need to ascertain that the patient has authorized the disclosure of the information and that there are no Federal laws

such as the Alcohol or Drug Abuse Act that would cover that particular disclosure.

And then, of course, have to look in terms of what the current statute or regulations in the particular State are. So it is difficult and that is why I think everyone here strongly supports the need for some uniformity.

Mr. CONDIT. The bill gives doctors discretion to disclose some health information to a patient's next of kin. This reflects current practice where doctors exercise judgment about what to tell a patient's spouse, except where the patient has objected.

This section has been quite controversial. Do we need to have a written authorization before a doctor can make a routine disclosure to a spouse?

Dr. LEWERS. This is a very difficult area. And I deal with it on a daily basis as a practicing physician. I think in general it is accepted, as you said, that we do release information to the next of kin, to the legal next of kin. The problem gets in where there is separation between spouses, and individuals who are not living with an individual who still legally is the next of kin, and sometimes that gets very hairy.

I've been in practice 25 years. I've only had two instances where an individual has come to me and said I do not want you to release information to my family, to my spouse, any information.

I get that in writing and document it and then hold it. And as a matter of fact have locked those records. But I don't see that as a big problem. It may be a larger problem as time goes on and perhaps we have more problems with social issues of separation, et cetera. But at this point, it's one we have been able to work with.

I'm not sure you need to try to get into that. That's going to be very complex and difficult, I would think, to write. And it would make more of a hassle to us in again making sure that we have that information; how often are you going to update it, et cetera.

Mr. CONDIT. So your response would be we do not need a written authorization?

Dr. LEWERS. My feeling is that we do not, at this point. I don't think it's that much of a problem. We run into it every day, we deal with it every day, and I don't think you need to put it into law.

Mr. CONDIT. Anybody else, anyone else have an opinion about that?

Mr. GIMPEL. Yes, the WEDI model suggests that no written authorization is necessary if the disclosure is to a member of the immediate family or to any other individual whom the person is known to have a close personal relationship, if it's made in accordance with good medical or professional practice, unless the disclosure is expressly limited or prohibited by the patient.

In other words, we put the onus on the patient to prohibit or limit the disclosure. Otherwise, it can be made in certain circumstances.

Mr. CONDIT. Your suggestion is the patient tells the doctor I don't want anybody to know about this?

Mr. GIMPEL. That's correct, that would prevent the disclosure.

Mr. CONDIT. Then he's bound by that, not to release the information?

Mr. GIMPEL. That's correct.

Mr. CONDIT. Anyone else have any views on this?

Let me ask about the effective date. The bill puts off the effective date for a few years to give everyone present plenty of time to learn the new rules.

We could shorten the period or delay or even phase in some parts. So what would be your preference?

Dr. LEWERS. Our feeling is that I believe the date is 1997. We think it's going to be very difficult to get everything promulgated by that time, and done so without really putting an imposition.

We have been able, voluntarily through physicians, to increase the number of physicians that are computerized. Right now, it's approximately 50 percent. I believe it's 49 point something. And that's growing rapidly, it's growing rapidly in rural areas which was the one area we were concerned it would not grow under a voluntary method.

I think forcing the physician community to get into the hardware issue, the software cost at this point in time, would be one of the major problems in moving your timeframe up. We think that the process, as I mentioned, should be through the negotiated rule-making.

We think that's going to take some time. There is no question the industry is moving very rapidly. There is a "smart card" now available somewhere here on the east coast. And so these issues are out there.

But I think that we need to be very careful that this is done and done properly, and so we would say that we could stay with the 1997 deadline at this point in time.

Mr. CONDIT. Anyone else care to comment or does everyone agree with that?

Mr. GIMPEL. WEDI believes that in order to move to an electronic data environment for health care, which is necessary in order to achieve the kinds of administrative savings and efficiencies that we envision, we need this quickly, as quickly as possible. And accordingly, we would urge that the effective date be shortened to the closest possible time consistent with the ability of industry to gear up to the necessary privacy standards.

Mr. CONDIT. So there is a little difference of view here.

Dr. LEWERS. Well, I'm not sure there's a difference of viewpoint. I guess my viewpoint is that I think the average time to promulgate regulations is almost a year, and if we're going to move through an area to do it any—I think your date is probably as quick as you're going to do it.

I would agree if it is feasible to get it done and get it done reasonably without putting a burden on the community, that should be done. But I think at this point in time you're just not going to be able to achieve it. That's—we're not, I don't think, in disagreement, it's just a date in time.

Mr. CONDIT. Do you agree that you're not in disagreement?

Dr. LEWERS. Agree to disagree.

Mr. GIMPEL. Mr. Chairman, I don't think we necessarily disagree on the overall concept. Perhaps the mechanism can be sped up by moving up the effective date of the act, but then, of course, until the regulations are in place, nothing can happen.

And by providing appropriate guidelines for promulgating regulations in the act, the promulgation of regulations can be effected we think relatively quickly, recognizing the slowness of government in this very important area.

We do agree, however, with the negotiated rulemaking process. WEDI has a provision that permits that and certainly calls for input from industry in the development of implementing regulations. We would definitely agree with that. But move it up as much as possible.

Mr. CONDIT. So what you're telling me, recognizing the slowness of government, if we move up the date, then it comes out about right for Dr. Lewers then.

Mr. GIMPEL. That may well be.

Mr. CONDIT. I want to recognize my colleagues who have joined us and we appreciate them being here, Mr. Stupak and Mr. Horn.

I am going to turn to Mr. Horn and ask if he has any opening statements and if he has questions, he could take this time to do it.

Mr. HORN. Thank you, Mr. Chairman.

Let me proceed to questions. With the previous panel, a few weeks ago, I asked about the problem of the disgruntled employee. I guess, Mr. Entin, since you represent hospitals, that's where that's most likely to occur, although it could occur in doctors' offices, where somebody takes information on a celebrity patient, releases it, as was testified here by one of our colleagues in a political campaign.

How much of a problem is that now?

Under this bill, does it create any more of a problem in terms of pinning the responsibility more on the institution than on the individual that does the deed?

Does that bother you?

Mr. ENTIN. No. I think that the responsibility for maintenance of security of this information ought to be shared both by the institution—which has an obligation to establish appropriate protocols and procedures, and to engage in effective training of staff so that the inadvertent type of disclosure can be avoided—and by the individual. The disgruntled employee who wants to have access and make a disclosure, I'm not sure that we'll ever come up with a fail-safe process for it.

But I think the major focus—and what the bill does is to place appropriate responsibilities on all of us who are responsible for holding this very important information and setting forth—the kinds of procedures that are necessary to ensure that inadvertent disclosure and inappropriate disclosures don't occur.

Mr. HORN. There's no real way you can protect yourself against an employee in the records room, any time of night or day, 24-hour operation, I assume, in a hospital, taking that file, running a Xerox, you'd never even know about it.

Mr. ENTIN. I would agree. I think if someone wants to do it, they'll find a way to do it.

Dr. LEWERS. That happens in the doctor's office as well. It's an area of concern that when we testified here, I believe it was last summer on this bill, it was one of our major concerns. It's not only

that, it's the changing of the medical record, the alteration of the medical record.

That's why we have held very tightly to the issue that these records must be secure. We've got to make sure that we work and deal with the industry to see that security is there. This occurs now.

I think that some of the penalties that you have placed in this bill would be helpful in deterring some of that, but we will never be able to get it completely out. And we could give you example after example where it has occurred.

Mr. HORN. Well, do you feel the penalties provided and the general mandates provided are sufficient or should there be more specific language of a different nature? Because some might argue that anything we write into the bill is directed at the people you can easily find responsible, as opposed to those that might be doing the damage.

Dr. LEWERS. As I understand what's been written in the bill, I think they are appropriate, at least as a start. No matter how high you get, you're never going to be able to take everybody out of that picture. I think that is appropriate.

There are no questions that in offices and in medical records there are what we call "moles." And we discover one every now and then. And we've got to be able to attack that individual. I think you've given us a role to do that.

Mr. HORN. Dr. Lewers, you mentioned you practice in Maryland.

Dr. LEWERS. Yes, sir.

Mr. HORN. And do you have patients from three States or so in the process?

Dr. LEWERS. I have patients that come to me from Delaware in particular, Virginia, since I'm on the Eastern Shore of Maryland. I still am fortunate enough to have some who have followed me from the district. So I basically deal with the three areas in those three States, yes, sir.

Mr. HORN. On the case of describing to the next of kin what the patient has, do you fall solely under the laws of Maryland when you practice in Maryland, or do you fall under the laws of other States where you do not physically practice?

Dr. LEWERS. As far as I am concerned, I practice under the laws of Maryland. If they come to me in Maryland, they are going to work under my laws, I would assume. One of the areas that we've had a problem in Maryland with, the issue that through the law was changed in Maryland, I believe it was 3 years ago, is whether or not an insurance company that is sitting in Illinois is complying with the laws in Maryland.

I'll get release of information forms from, you know, an insurance company in Illinois, which do not comply with the laws in Maryland. And we've had some problems trying to figure out whether we release that information or not and getting compliance there.

So from my understanding, they need to comply in Maryland, but they don't know about it. That's why we really—I think every one of us here, and I think you will hear it in the second panel, too, go for this preemption issue. We need to standardize.

Mr. HORN. In other words, you want a national standard.

Let me take the case of AIDS. I know the California law sometimes makes no sense on the subject, as I last remember it. And maybe my colleague who was in the legislature will know much more about it. But what is the Maryland rule if a wife appears and the male patient has AIDS, can you notify her?

Dr. LEWERS. We have to when we deal with—the law in Maryland is very, very strict on that. Even for notification of an individual or even to do the testing, I must sit down with that individual, I must counsel that individual. We have separate forms for the AIDS patient. After the testing is done, I have to sit down and counsel them. Part of that counseling is whether or not that information would be released and to whom that would be released. So it is very detailed.

I don't do a great deal of AIDS work, so I'm not totally up on the exact details of it, but I know each time I get around to testing, I pull that little form out and I review it very carefully.

Mr. HORN. Under Maryland law, can a male who has AIDS refuse to have you release that information so his spouse is informed of that?

Dr. LEWERS. I would have to review that. I can find out and I'll let you know. I know that he cannot refuse for us to release it to the public health bodies. But whether or not the law goes into that element, I don't recall and I'd have to get back to you. I'll try to find that and let you know.

[The information provided by Dr. Lewers is contained in the subcommittee files.]

Mr. HORN. Well, I'm rather concerned when a spouse is not informed on that and you get—as I recall, we went through some of that in California.

Let me ask you, in this legislation, we're talking about alternate dispute resolution panels. What do any of you think, all of you, about the mechanism?

Is it sufficient in deterring, say, frivolous lawsuits? Or should a provider receive a one-time notification first before civil monetary penalties can be pursued for failure to comply?

Do you have any feelings on that?

Mr. ENTIN. I'll take a crack at it.

I think that alternative dispute resolution has as its objective to take most disputes which can be and should be resolved without resort to court, and to get them resolved at a level where they should be. And so to the extent that that is the purpose of the inclusion of that in this legislation, I think that it's an appropriate piece of the bill. And certainly is well-meaning and seems to make a good deal of sense.

Mr. HORN. OK. Any other reaction?

Yes, sir, Mr. Gimpel.

Mr. GIMPEL. WEDI would agree in that in the WEDI model we provided for the promulgation of alternative dispute resolution methods. My reading of section 163 of the bill is that the alternative dispute resolution systems or methods don't go to the assertion of civil violations or criminal violations by the Secretary, but are designed to handle disputes between the various private entities that might arise from an unauthorized disclosure.

Mr. HORN. Any other reaction?

If not, let me ask, H.R. 4077, has three different trustee categories, and the question is would it be more helpful to have one category and separate the providers' responsibilities by function?

Did you have a chance or your staff have any chance to look at that particular aspect?

Mr. ENTIN. If what the Congressman means by "function" is the use of the data, that is our suggestion, our recommendation. I think it's a simpler approach to take.

You start with the basic set of responsibilities and standards and then you recognize that public policy might dictate that there's certain exceptions that ought to exist, which are predicated on the use of the information and go that way. So I think that is a more workable approach.

Mr. HORN. OK.

Dr. Lewers, since you're testifying for the American Medical Association, some of these proposals that are before Congress now include provisions that permit, say, a medical society in a particular State to participate in disciplinary activities. And the question would be is this type of legislation helpful in assisting the Secretary to determine compliance with confidentiality laws?

Dr. LEWERS. You're talking about 4077?

Mr. HORN. Well, I am talking really about different health care proposals and their mechanisms. Just what do you think about that?

Dr. LEWERS. We think that medical societies, organizations, should be able to deal with this and work with discipline without fear of retribution, as has been in the past. As you, I am sure, are aware, there have been some recent regulations which have freed up the society, particularly in fee disputes. And we certainly support that.

We feel that there are areas that have been very restrictive at this point in time. Within the fee dispute area, for example, I used to sit in Maryland on a commission in which we routinely had fee complaints and brought physicians before us, and discussed the fees that were out of line. But we had to stop doing that. And we had to stop doing it because of the fear of antitrust and antitrust suits which were filed in Maryland. That now has been clarified. So any way that we could do that so we can deal with true peer review would be welcomed.

Mr. HORN. OK.

Any other comments on that?

Last question, records retention in terms of medical records. What are the laws of Maryland and what's your experience generally with the number of years one must maintain those records? And does it vary by purpose?

Let's say there was a murder investigation. Well, one's whole life one can be charged with murder in most States. There's no statute of limitations. If there are other criminal investigations, you have particular statutes of limitations.

So what's your reaction to the degree to which there should be a preemptive period and what should that period be?

Dr. LEWERS. It does vary from State to State, you know, as to how long you legally hold on to them. Primarily for liability issues, which is an area we'd love to see some changes in.

Quite frankly, I never throw a record away. I would never get rid of a record. And when I speak on this around the country and I advise physicians, find some place to put them, but don't throw them away. That is our record of service. It is the one thing that's going to protect us in many instances. So I never get rid of a record. Even though there are laws saying you can do it at this point, our recommendation is hold on to them.

Mr. HORN. Any other reaction to that?

Hospitals have any feelings on that one way or the other?

Mr. ENTIN. Well, I think it becomes a problem of just a sheer storage problem. And from my prior life—I can't say that I disagree with Dr. Lewers.

In my prior life, when I defended some medical malpractice actions representing hospitals in Cook County, IL, we were dealing with cases that were 10 and 12 years old. Often the medical record is the only piece of evidence you have to reconstruct what happened. So speaking personally, I'm reluctant to see too much thrown away.

On the other hand, I do recognize that for hospitals with hundreds of thousands of patients that come through, you just become overburdened with the enormous weight of paper. So some reasonable accommodation needs to be made, and I think you have to then balance that against the other legitimate uses of the information that might arise at a later time and not penalize those of us who are in the health storage conundrum with having to alter or destroy records.

So I think some reasonable accommodation has to be made. We cannot hold on to everything forever, despite my personal preference that we do that as well.

Mr. HORN. Well, with computer technology, it will put probably all the records that would fill this room on a CD disk, as we know. Being from Cook County, I thought they only threw away the death certificates, people live to 200, so they could vote.

Mr. GIMPEL. I was only going to add that as we move toward an electronic data environment, the storage problem we hope would be less of a problem, as the Congressman noted.

Mr. HORN. Sure, thank you.

Mr. CONDIT. Thank you, Mr. Horn.

Mr. Stupak, if you want to make an opening statement, you're welcome to do that. You can ask any questions you like.

Mr. STUPAK. Thank you, Mr. Chairman.

No opening statement, but I'd like to pick up where Representative Horn left off. What about dead people, how long do we hold those records?

Is it when they die, they can be released? Does the estate, do you have to get authorization from the estate?

How would that work underneath this proposal? Should you hang on to them for 2 years or does the privacy end upon the death of an individual?

Ms. FRAWLEY. Well, I'd just like to comment, the one thing H.R. 4077 doesn't really discuss, decedent's records as all. Currently, that is a problem where a request for information is received after a patient has expired and individuals are struggling to determine who should be the appropriate individual to authorize the release,

whether it's the next of kin, whether it's the executor, the administrator.

I certainly think that we need to address decedent's release of information. I don't believe that we should set up different standards for records in terms of retention.

I think we recognized right now that we don't have a uniform retention standard for any medical records in this country. It does vary from State to State.

I would caution the subcommittee from setting up different standards for minors versus decedents, and so forth. I think that way we would just be back into a conundrum again of having all kinds of conflicting guidelines.

So I think where we can establish some uniformity certainly in terms of retention, establishing standards in terms of rights and responsibilities in release and information, that would be appropriate. But I do think the fact it's unclear as to how decedent's records are handled by this bill is something we need to explore.

Mr. STUPAK. OK. Anybody else on that one?

Dr. LEWERS. I would not want to see them released. I would agree, we should not handle them differently. I think they are available—one of the very, very key issues of holding on to records are some of the research programs. And so you can go back as long as you don't identify the individual and bring that out.

I once did a study at Georgetown where we went back 15 years and it has been a study that has stayed, and I did that in the late 1960's. Because we had information that went back on a certain disease process 15 years, we were able to do some prediction on what was going to happen to those individuals. So I wouldn't want to see those records destroyed.

Now they may be on microfilm or now they may be on a CD, but let's be able to get do them. Let's not get rid of them and let's not release them.

Mr. STUPAK. Well, doctor, you lead to my next question.

You know, there is public support for research. However, there's always the concern about medical research generally and what are the information being used for, whether they are living or deceased members. Identifiable records which identify individuals, how can we continue to have some protection but yet allow research access to those records that they need for the research?

Dr. LEWERS. I think in—we just cannot allow for the individuals to be identified. There's got to be some way for that to be secured, and as you go in the aggregate, which is what most research is going to do. Other than that, the individual or some representative is going to have to give a release for that information to be evaluated. I don't think we can do it any other way.

Mr. STUPAK. Let me jump to the next stage of it then.

A lot of people suggest that we use Social Security numbers as health identifiers. Social Security numbers, just about everybody have access to them nowadays. What's your feelings on that?

Is the Social Security number, does it really matter? What numbers should we—some other methods that you would use?

Dr. LEWERS. Some other number. We feel that the Social Security number is available everywhere. And it's just—it is not a secure number, so we feel there should be a unique identifier.

When it comes to physicians, that's fairly easy, because we have an identifier and educational number that we have on every physician, whether or not the individual is a member of the American Medical Association or not. They have a number.

There's no other entity in the country that has that on physicians. We're very willing to work with anyone to provide that.

When it comes to an individual, we do not feel it should be the Social Security number. It should be a separate number.

Mr. STUPAK. OK.

Do you—your number, much like us attorneys, we have identifiable numbers, but do you disclose them then when you order medical books or research?

Dr. LEWERS. No.

Mr. STUPAK. OK.

Is there any provision in this bill which would allow an individual to go to a health care provider and obtain a list of the legal entities that were provided health information and under what authority that information was obtained?

In other words, if I wanted to go to my local hospital, could I go in off the street and say I'd like to know everyone who you disclosed information about me on?

Dr. LEWERS. I'll get the hospital answer that.

[The information provided by Dr. Lewers is contained in the subcommittee files.]

Ms. FRAWLEY. Section 111, which is the inspection of the records, clearly provides an individual the right to find out from any health information trustees, the bill as currently drafted, the accounting for disclosures. And so basically that would allow an individual to go to a hospital and ask who has had access to their health record and to see what disclosures were made.

Now, that's important because of the concern that information is disclosed, and one of the major concerns that we've all talked about this morning is the issue of redisclosure. So information could be disclosed, you know, to an insurance carrier, or to your employer, and then the concern is you would like to know that, and therefore be able to go to that individual and find out if they have used that information, who has had access to the information. So I think section 111 does address that concern.

Mr. STUPAK. See, when I read 111, I felt that it required the health provider to maintain a log of, if you will, of who they disclosed it to, but I didn't see anything in there which would guarantee that the private individual would have the right to go in and request who have you disclosed it to. And we're talking about individual reports and individual privacy rights here, I would fall on allowing the individuals to go into any health care provider to obtain that information.

I can go through a number of examples where it's happened in the past in Michigan where people were not provided that information and information being used improperly, and it's difficult at times to ascertain, especially when you are asking us to give up some private rights. So I think that would be one section I'd want to improve upon. Especially when you speak of health records, you know, it also includes mental health and that's where it gets a little difficult.

The chairman asked about the cost of transferring health data, especially in the computerized environment, and I think, Dr. Lewers, I think you said that about 49 percent of the rural physicians are probably up to speed on this.

Dr. LEWERS. All physicians, 49 percent of all physicians currently have computerized systems. It's growing rapidly in the rural area, faster than we thought it would, but the 49 percent figure are all physicians in the country.

Mr. STUPAK. Is that an expensive proposition, to obtain the networking? I think we're going to have a nationwide network, electronic, would that be an expensive burden, say, on rural physicians? If so, is there any incentives to help them make that transition?

Dr. LEWERS. It is expensive. When I computerized my office, it cost me \$20,000 by the time I had all the hardware, the network and the software, et cetera. And the yearly cost of doing that business is not, you know, inexpensive. So yes, it is very expensive.

Are there ways and incentives to bring that into line? The American Medical Association has been working on some endeavors to sort of do group purchasing and dealing with a couple vendors to help provide certain issues, but as far as other incentives, that becomes exceedingly difficult because of some of the changes that are required and the systems that are required around the country.

So we've not been able to get into that to any great degree, but it is expensive. It's an area that we have grave concern. That is one of the reasons why we want to—while we recognize the need to move quickly, we don't want to move too quickly because of putting an undue cost burden on the provision.

Mr. STUPAK. One more question.

The administrative subpoenas, as they call it in the bill on page 47, you can't get a good definition. In your estimation, what would an administrative subpoena be—put forth by a governmental agency, strictly a State public health department, a local county health department, inspector general, IG; how would you define that broad term, administrative subpoena?

Mr. LEWERS. I would not have any idea. I would refer to legal counsel to define it for me.

Mr. ENTIN. When I saw the provision, I just assumed that it is a subpoena issued pursuant to authority granted to agencies, not judicial bodies. And various agencies do have the power of subpoena in order to conduct their business.

I assume that is what this is referring to, but I didn't draft the bill.

Mr. STUPAK. It would not be limited to the Justice Department? We would go all the way down to a local public health department?

Mr. ENTIN. Or a department of health.

Mr. STUPAK. In Michigan we have one way. I am sure California and Maryland and others have different rules for administrative subpoenas. They can be very tight and broad and that is where I feel abuse sometimes comes in.

Thank you.

Mr. CONDIT. One last question. At the last hearing we heard testimony that the public is opposed to use of health records for direct

marketing. How do we control use of health records for direct marketing? Are there some types of marketing we should allow?

I am not offended if a doctor mails to all the patients that he is moving his office, but what about hospitals starting an obesity clinic? Can they tell all patients or use their records to identify obese patients? Do any of you have any feelings about the use of this information, the selling of the list? Where do we draw the line?

Mr. ENTIN. We draw the line at selling of lists. That is something that should not occur. We have various advisories and documents that have been developed over the years that we disseminate to our members with regard to the overall question of confidentiality of records and use of records for a variety of purposes.

I have reviewed those. I can't say that we have a direct position that opposes marketing in general. One could justify use of patient information in a hospital to the extent that the hospital is using that list of patients to inform them of services that are beneficial to members of the community.

To go beyond that and to target patients for particular services because of their disease condition probably is something which doesn't need to be asked. It is a very difficult problem and you have to balance, I would suggest, the need to provide useful information to the community against the right to privacy.

Mr. CONDIT. Anyone else?

Mr. LEWERS. I think we agree. We still have to fallback to where we were as far as unique identification and associating that individual with release of that information. Sending an individual a letter is one thing but if you are using that information in identifying that patient, that is wrong.

There are a lot of times where you need to get disease-specific information for tracing issues, certain diseases where you may have to go into that. But to market is a little different area that we have to be careful about, and I would agree with the previous speaker on that.

Mr. CONDIT. Do you have comments or just agree—

Mr. GIMPEL. We didn't deal specifically with that issue so I don't have particular comments on it. We think that the privacy protections afforded are probably adequate to control that kind of situation.

Ms. FRAWLEY. I concur with Dr. Lewers and Mr. Entin. I think that any use of an individual's information for direct marketing purposes should be authorized by that individual. I think we have to be very careful about those kinds of practices.

Mr. CONDIT. Thank you. We will call upon you for additional information.

Thank you very much for your time. We appreciate it.

Panel 2 is Dr. Barker, Dr. Sepulveda, Mr. Bolan and Professor Schwartz. We have a brief delay.

If you would have a seat.

If you would all stand and raise your hand.

[Witnesses sworn.]

Mr. CONDIT. Thank you very much. We appreciate you gentleman being here this morning. Dr. Barker.

**STATEMENT OF RICHARD BARKER, M.D., PRESIDENT,
HEALTHCARE INDUSTRIES, IBM CORP., ACCOMPANIED BY
MARTIN SEPULVEDA, M.D., DIRECTOR, OCCUPATIONAL
HEALTH SERVICES**

Dr. BARKER. Good morning Mr. Chairman and members of the committee. My name is Richard Barker and I am president of healthcare industries for IBM.

Accompanying me today is Dr. Martin Sepulveda, IBM's director of occupational health services. We are pleased to be here today to help you address this very important topic of privacy.

You have asked for our views on H.R. 4077, as an information technology company and as an employer.

I have responsibility for IBM's strategy for the health care marketplace and for helping our customers work through the very real transformation occurring in the U.S. health care system.

Dr. Sepulveda is responsible for IBM's occupational health services and programs and, consequently, he will speak to the issues of health information privacy from the company's role as an employer.

IBM is seeing first hand the significant change taking place in health care as we work with customers, change driven principally by market forces rather than policy considerations.

We see the central role information systems are playing in this process as these stakeholders deal with cost, access and quality issues. Data standards and data security are the two major roadblocks to building the health care information highway. Both must be tackled with urgency.

As a self-insured, multistate employer, providing health benefits to over 525,000 people across the country, we see the expanded and valuable role user friendly health-related information is playing.

From both of these capacities, we know the importance assigned to the issue of privacy by the public and various health care stakeholders. We believe there is a general desire by health care professionals and others "to do the right thing" with the health information they handle, if for no other reason than a sense of respect for the individual and fairness.

However, they also sense that a wider dissemination of health care data would improve productivity. The dilemma we all face is striking the right balance between the interests of the individual and the health care "learning process."

We feel H.R. 4077 is an excellent starting point in this regard. It sets up a uniform set of comprehensive Federal privacy rules, and very importantly, it takes a flexible approach to compliance rather than a prescriptive one. We commend you and your staff for this and consider it a major strength of the legislation.

To a great extent, the U.S. health care system began transforming itself before the most recent widespread attention to health care reform took hold with the public and policymakers. Many stakeholders have been changing their traditional approaches in order to improve efficiency and to reduce cost.

However, because our health care system is so large and involves so many players, the sum of these individual initiatives has still not achieved the transformation in health care productivity that we all seek. The public has sensed this shortfall between performance

and potential and agrees there is a need for some kind of systematic reform.

IBM agrees, and we applaud the President and those public officials who are trying to enact comprehensive health care reform in 1994.

One area that needs to be addressed by systematic reform is the building of an integrated health information infrastructure. Systems are needed to enhance the operation of various stakeholders independently and to enable them to work together more efficiently for the betterment of patients and consumers.

It is critical to remember that the common denominator in our health care system is the individual. The individual's information is the essence of health care, and health information systems must be regarded by individuals as secure enough to benefit, not undermine, their health care needs.

Efforts to develop and establish new health care information systems are broad based. In our written statement I refer to a number of examples.

Health care data bases of all kinds are already being built to ensure continuity of care to the patient and the benchmarking of outcomes across the system. It is very important that we provide a clear and uniform legal framework for these efforts.

The health care system of today is composed of natural medical marketplaces not bound by State borders. This reality gives rise to the need for Federal uniformity in the governing of health information. H.R. 4077 helps accomplish this.

It is clear that the public places great importance on the confidentiality of health records. At IBM, we have considered privacy of individual information of paramount concern for decades.

We continue to be reminded of this as we work with segments of society that rely heavily on information technology. Our expertise in maintaining data security has helped us to address this concern.

Uniform privacy rules like those in H.R. 4077 are needed if we are going to assure all Americans that their health-related needs are being advanced, not threatened, and to reap the benefits of the broad-based efforts referred to in our written statement. Without them, the development of an electronic health information system envisioned by the President and others, such as Representatives Sawyer and Hobson, will be in doubt and its value greatly diminished.

Mr. Chairman, I would like to ask Dr. Sepulveda to speak to the role of the employer as a provider of health benefits and as a privacy "trustee," to borrow a coined phrase.

Mr. CONDIT. Dr. Sepulveda.

Dr. SEPULVEDA. Thank you, Mr. Chairman.

The President and most Members of Congress propose reforming the health care system by continuing to use the current employment-based system as the basis for the future. IBM agrees with this approach.

We believe employers play a very constructive role in today's system. Consequently, any health care reform bill enacted should strengthen the roll of the employer, not diminish it.

Employers' benefit plans generates and use much of the health information that flows through the health care system today. In turn, employers have a very keen interest in the privacy issue.

They have the need to balance access to individual information for appropriate business needs with an individual's right to privacy. Employees in turn need to have strict assurances that the privacy of their medical records will be protected by their employers.

To be of benefit, privacy legislation, such as H.R. 4077, should not tie the hands of employers so severely that they lose the flexibility to perform these necessary functions. IBM has maintained a very high standard with respect to ensuring the confidentiality of information entrusted to it.

The company's interest dates back to the 1960's when our privacy policies were formalized due to our desire to respect our individual employees and a general public apprehension about the effects of computers.

Let me take a moment to share with you our privacy principles relevant to employee personnel information. They are as follows:

To collect, use and retain only personal information that is required for business or legal reasons; to provide employees with a means of ensuring that their personal information in IBM personnel records is correct; to limit the internal availability of personal information about others to those with a business need to know; and to release personal information outside IBM only with employee approval, except to verify employment or to satisfy legal needs.

These principles apply to all personal information but have particular meaning for medical information which, I believe, deserves the greatest degree of protection. IBM access to confidential medical records is limited to IBM medical staff and department personnel under their immediate supervision. They will provide access only: To benefits plan administrators who may review information needed for determining eligibility for benefits; to others with a need to know to evaluate medical recommendations, medical restrictions and accommodations as they relate specifically to the work environment and the ability to perform the job; and to legal counsel when medical status or information is at issue or required.

All employees at IBM may obtain copies of their records from the IBM medical department. Further, with few exceptions, we require our medical staffs to obtain prior approval of the employee either before disclosing or seeking confidential medical information.

In addition to the information which is contained in our own internally generated medical records, we have placed restrictions on our benefits contract administrators on how employee benefits information can be used and even what information they will pass on to us at IBM.

For example, our IBM plan administrators receive only aggregate data derived from medical records available to the carriers which does not permit linkage of any individual employee with a particular medical condition.

We believe the objectives of H.R. 4077 are well-grounded. They fundamentally agree with our company's privacy principles and practices. They strive to create a balance of purpose.

The general responsibilities outlined in your bill for health information trustees are consistent with the responsibility we have placed on ourselves at IBM.

Dr. BARKER. You have embarked upon a difficult but very important challenge and we look forward to continuing our work you.

I would like to highlight a few of our comments included in our written statement regarding your legislation and leave the rest for later discussion.

The concept of a health information trustee, we believe, is a good one and preferable to the concept of an owner of health-related information. We believe questions of ownership are less tractable, and ultimately less relevant than those of access.

We think some clarification would be helpful relevant to the definition of "relating to the provision of and payment for health care." Dr. Sepulveda can elaborate, if you would like, on this point.

Let me note for the committee that an employer's obligations under the Occupational Safety and Health Act [OSHA] require the submission of information to "OSHA logs." These logs are publicly available information with open right of access to anyone.

They contain personal identifiers and, increasingly, diagnostic information. Our question would be, "Is this 'protected health information' and, if so, how are the trustee obligations of safeguarding privacy to be met?"

Relative to sections 114 and 115, regarding accounting for disclosures and security obligations imposed on health information trustees, we believe this is an area where available information systems and technology, such as "smart cards," can actually enhance compliance and the confidentiality of medical information. Audit trails on how information has been assembled and accessed are more readily available in an electronic format than in a paper one.

This raises a suggestion we would like to offer affecting section 153 in subtitle D, standards for electronic documents and communications. We don't believe the government should set the standards.

We would encourage the committee to modify the wording on page 64, line 5, to read: "shall establish standards in consultations with appropriate private sector standards organizations."

This change would be consistent with other health care reform legislation, in particular H.R. 3137 introduced by Representatives Sawyer and Hobson.

In conclusion, Mr. Chairman, we appreciate having been given the opportunity to offer our views on the general issue of health information privacy and H.R. 4077 specifically.

IBM is committed to enacting health care reform this year. Your legislation makes an important and valuable contribution to the reform effort. We welcome the opportunity to work with you and others in the months ahead.

Mr. CONDIT. Thank you.

Dr. Barker, your suggestion is a good one and we will do that. Thank you.

Dr. Sepulveda, did you have additional comments?

Dr. SEPULVEDA. No, Mr. Chairman.

[The prepared statement of Dr. Barker and Dr. Sepulveda follow:]

Statement of

Dr. Richard Barker

President, Healthcare Industries

and

Dr. Martin Sepulveda

Director, Occupational Health Services

International Business Machines Corporation

on the

Fair Health Information Practices Act of 1994

before the

Committee on Government Operations

Subcommittee on Information, Justice, Transportation and Agriculture

United States House of Representatives

May 4, 1994

EXECUTIVE SUMMARY

You have asked for our views on H.R. 4077, the Fair Health Information Practices Act of 1994, as an information technology company involved with the increasing computerization of health records and as an employer.

In both of these areas, we know the importance assigned to the issue of privacy by the public and various health care stakeholders. We believe there is a general desire by health care professionals and others to do the right thing with the health information they handle, if for no other reason than a sense of respect for the individual and fairness. However, they also sense that a wider dissemination of health care data would improve productivity, as experience is shared and the medical community converges on best practice treatment regimes. The dilemma we face is striking the right balance between the interests of the individual and the health care 'learning process.'

We feel H.R. 4077 is an excellent starting point in this regard. It sets up a uniform set of comprehensive federal privacy rules for people who handle health information to know what "the right thing" is. Very importantly, it also takes a flexible approach to compliance rather than a prescriptive one. We commend you and your staff for this and consider it a major strength of the legislation.

Transforming The Health Care System

One area that needs to be addressed by systematic reform is the building of an integrated health information infrastructure. Systems are needed to guide and enhance the operation of various stakeholders independently and to enable them to work more efficiently together for the betterment of patients and consumers. It is critical to remember that the common denominator in our health care system is the individual, whether as a patient, family member, consumer, or citizen. The individual's information is the essence of health care, and health information systems must be regarded by individuals as secure enough to benefit, not undermine, their health care needs.

Health care databases of all kinds are already being built. In addition to physician and hospital records, ISCs are assembling their own clinical data repositories to ensure continuity of care to the patient and the benchmarking of outcomes across the system. Some states, notably Minnesota, are starting to build statewide repositories to accelerate health care reform. It is very important that we provide a clear legal framework for these efforts.

The health care system of today is composed of natural medical marketplaces not bound by state borders. This reality gives rise to the need for federal uniformity in the governing of health information,

especially as we strive to improve the financing and delivery of care using administrative and clinical information systems. H.R. 4077 helps accomplish this.

The Importance of Privacy

Privacy is a social issue that we all must address. It involves balancing the rights of the individual with the needs of society. It requires choices about the kinds of personal information that are allowed to flow into and through record keeping systems, electronic or paper. It deals with the type of information collected, how it is used, and how long it is retained. As we try to find the right policy balance, we need to assume that once aware of what the ground rules are, most people and organizations will comply with them. On the other hand, we must be realistic and actively monitor for compliance by all.

Uniform privacy rules are key if we are going to assure all Americans that their health-related needs are being advanced, not threatened. To reap the benefits as a society of the broad-based efforts I mentioned above, a set of fair information practices like those in H.R. 4077 are necessary. Without them, the development of an effective and efficient electronic health care data interchange system envisioned by the President and others, such as Representatives Sawyer and Hobson, will be in doubt and its value greatly diminished.

The Employer's Role in Health Care

Employers today play a central role in our health care system. Most Americans and their families receive coverage through an employer. Self-insured firms like IBM actively design, manage, and fund health benefits for their employees. Employers are responsible for ensuring that a healthy and safe workplace exists at their facilities, and they underpin the nation's worker compensation system. To remove the employer from this active and central role would greatly disrupt the present system and remove many of the positive things employers choose to do, such as health prevention and wellness programs.

To be of benefit, privacy legislation, such as H.R. 4077, should not tie the hands of employers so severely that they lose the flexibility to perform these necessary functions. Employers need to have access to sufficient information to manage their workforce effectively and perform necessary research and analysis that requires medical information. Particularly detrimental would be severe limitations placed on the transfer of information between health care providers and employers at a time when new and better communications potential is being developed by community health networks.

IBM and Privacy

As an information systems and processing company, IBM has maintained a very high standard with respect to ensuring the confidentiality of information entrusted to it. The company's interest dates back to the 1960s when our privacy policies were formalized due to our desire to respect our individual employees and a general public apprehension about the effects of computers.

We believe the objectives of H.R. 4077 are well-grounded. They fundamentally agree with our own company's privacy principles and practices. They strive to create a balance of purpose. The general responsibilities outlined in your bill for health information trustees are consistent with the responsibilities we have placed on ourselves at IBM.

Conclusion

IBM is committed to enacting health care reform this year. Your legislation makes an important and valuable contribution to the reform effort. We welcome the opportunity to work with you and others in the months ahead.

Good morning, Mr. Chairman, and Members of the Committee.

My name is Richard Barker, and I am President of Healthcare Industries for IBM. Accompanying me today is Dr. Martin Sepulveda, IBM's Director of Occupational Health Services. We are pleased to be here today to help you address this very important topic of privacy and to think through its public policy dimensions.

You have asked for our views on H.R. 4077, the Fair Health Information Practices Act of 1994, as an information technology company involved with the increasing computerization of health records and as an employer.

I have responsibility for IBM's strategy for the health care marketplace and for helping our customers work through the very real transformation occurring in the U.S. health care system. Dr. Sepulveda is responsible for IBM's occupational health services and programs and, consequently, he will speak to the issues of health information privacy from the company's role as an employer.

IBM is seeing first hand the significant change taking place in health care as we work with hospitals, insurers, managed care organizations, employers, government and others--change driven principally by market forces rather than policy considerations.

We see the central role information systems are playing in this process as these stakeholders deal with the cost, access and quality issues of health care delivery and financing. Data standards and data security are the two major roadblocks to building the health care information highway. Both must be tackled with urgency, and we wish to do all we can to assist in both tasks.

Concurrently, as a self-insured, multi-state employer providing health benefits to over 525,000 IBM employees, retirees, and their families across the country, we ourselves see the expanded and valuable role user friendly health-related information is playing for us as a benefits provider and for our employees.

In both of these areas, we know the importance assigned to the issue of privacy by the public and various health care stakeholders. We believe there is a general desire by health care professionals and others to do the right thing with the health information they handle, if for no other reason than a

sense of respect for the individual and fairness. However, they also sense that a wider dissemination of health care data would improve productivity, as experience is shared and the medical community converges on best practice treatment regimes. The dilemma we face is striking the right balance between the interests of the individual and the health care 'learning process.'

We feel H.R. 4077 is an excellent starting point in this regard. It sets up a uniform set of comprehensive federal privacy rules for people who handle health information to know what "the right thing" is. Very importantly, it also takes a flexible approach to compliance rather than a prescriptive one. We commend you and your staff for this and consider it a major strength of the legislation.

Transforming The Health Care System

To a great extent, the U.S. health care system began transforming itself before the most recent widespread attention to health care reform took hold with the public and policymakers. Providers, payors, employers and even government agencies, to a degree, have been changing their traditional approaches in order to improve efficiency and reduce cost. However, because our health care system is so large and involves so many players, the sum of these individual initiatives has still not achieved the transformation in health care productivity we all seek. The number of uninsured has grown. Growth in costs, while moderating somewhat, has continued to exceed growth in consumer prices generally and there are concerns about quality of care in many areas of the country. The public has sensed this shortfall between performance and potential and agrees there is a need for some kind of systematic reform.

IBM agrees, and we applaud the President and those public officials who are trying to seize the opportunity and enact comprehensive health care reform in 1994.

One area that needs to be addressed by systematic reform is the building of an integrated health information infrastructure. Systems are needed to guide and enhance the operation of various stakeholders independently and to enable them to work more efficiently together for the betterment of patients and consumers. It is critical to remember that the common denominator in our health care system is the individual, whether as a patient, family member, consumer, or citizen. The individual's information is the essence of health care, and health information systems must be regarded by individuals as secure enough to benefit, not undermine, their health care needs.

Efforts to develop and establish new health information systems are broad-based. I'd like to mention a few examples.

Groups of constituents across the country are taking the initiative to build community level health information networks (CHINs) in order to share administrative and clinical information as they strive to lower cost and increase quality through electronic billing and outcomes measurements. IBM is participating in a number of these community-based efforts. The San Antonio Health Care Partnership is one such example.

Medicare and many large private-sector payors like Blue Cross and Blue Shield are aggressively pursuing electronic data interchange (EDI) to increase the speed of claims reimbursement and reduce their administrative cost. IBM is actively involved with the Health Care Financing Administration (HCFA) through our subsidiary Advantis and with Blue Cross/Blue Shield of New Jersey in efforts to advance the transmission of large volumes of electronic health information securely and at costs much lower than the corresponding paper-based transactions.

Health care providers are moving rapidly to develop integrated systems of care (ISC) in order to reduce overall operating costs and deliver more effective and higher quality care. Providers are finding that information systems are the essential thread holding these organized systems together so that they can be more competitive in their marketplaces. We are working with Kaiser Permanente in Colorado and Columbia Presbyterian Hospital in New York, among others, on these kinds of systems.

Health care databases of all kinds are already being built. In addition to physician and hospital records, ISCs are assembling their own clinical data repositories to ensure continuity of care to the patient and the benchmarking of outcomes across the system. Some states, notably Minnesota, are starting to build statewide repositories to accelerate health care reform. It is very important that we provide a clear legal framework for these efforts.

The health care system of today is composed of natural medical marketplaces not bound by state borders. This reality gives rise to the need for federal uniformity in the governing of health information, especially as we strive to improve the financing and delivery of care using administrative and clinical information systems. H.R. 4077 helps accomplish this.

The Importance of Privacy

It is clear that the public places great importance on the confidentiality of health records. The Equifax study portrayed this in a number of ways. It did so most starkly, however, by the findings showing that 85% of the public believe protecting the confidentiality of medical records is of critical importance in national health care reform, putting this ahead of other reform objectives such as expanding health coverage to the uninsured and obtaining better medical research.

At IBM, we have considered privacy of individual information of paramount concern for decades. We continue to be reminded of this as we work with segments of society that rely heavily on information technology to carry out their missions. Our expertise in maintaining data security has helped us to address this concern. However, we recognize that making information secure does not ensure privacy in and of itself.

Privacy is a social issue that we all must address. It involves balancing the rights of the individual with the needs of society. It requires choices about the kinds of personal information that are allowed to flow into and through record keeping systems, electronic or paper. It deals with the type of information collected, how it is used, and how long it is retained. As we try to find the right policy balance, we need to assume that once aware of what the ground rules are, most people and organizations will comply with them. On the other hand, we must be realistic and actively monitor for compliance by all.

Uniform privacy rules are key if we are going to assure all Americans that their health-related needs are being advanced, not threatened. To reap the benefits as a society of the broad-based efforts I mentioned above, a set of fair information practices like those in H.R. 4077 are necessary. Without them, the development of an effective and efficient electronic health care data interchange system envisioned by the President and others, such as Representatives Sawyer and Hobson, will be in doubt and its value greatly diminished.

Mr. Chairman, I would like to ask Dr. Sepulveda to speak to the role of the employer as a provider of health benefits and as a privacy "trustee," to borrow a coined phrase.

The Employer's Role in Health Care

Thank you, Mr. Chairman. The President and most members of Congress propose reforming the health care system by continuing to use the current employment-based system as the basis for the future. IBM agrees with this approach. We believe employers play a very constructive role in today's system and have helped

bring about many of the most innovative developments in health care delivery. Any health care reform bill finally enacted should appropriately strengthen the role of the employer, not diminish it.

Employers today play a central role in our health care system. Most Americans and their families receive coverage through an employer. Self-insured firms like IBM actively design, manage, and fund health benefits for their employees. Employers are responsible for ensuring that a healthy and safe workplace exists at their facilities, and they underpin the nation's worker compensation system. To remove the employer from this active and central role would greatly disrupt the present system and remove many of the positive things employers choose to do, such as health prevention and wellness programs.

Employers' benefit plans generate and use much of the health information that flows through the health care system today. In turn, they have a keen interest in the privacy issue. They have the need to balance access to individual information for appropriate business needs with an individual's right to privacy. Employees, in turn, need to have assurances that the privacy of their medical records will be protected by their employers.

Employers regularly play three distinct roles relevant to the provisions of H.R. 4077. They act as:

- * Providers of health benefits and payors of health claims
- * Providers of emergency care when necessary, and
- * Stewards of a healthy and safe workplace to ensure the well-being of their employees.

To be of benefit, privacy legislation, such as H.R. 4077, should not tie the hands of employers so severely that they lose the flexibility to perform these necessary functions. Employers need to have access to sufficient information to manage their workforce effectively and perform necessary research and analysis that requires medical information. Particularly detrimental would be severe limitations placed on the transfer of information between health care providers and employers at a time when new and better communications potential is being developed by community health networks.

IBM and Privacy

As an information systems and processing company, IBM has maintained a very high standard with respect to ensuring the confidentiality of information entrusted to it. The company's interest dates back to the 1960s when our privacy policies were formalized due to our desire to respect our individual employees and a general public apprehension about the effects of computers.

In the 1970s, we conducted a comprehensive review of specific internal guidelines and began management training programs to support compliance with these guidelines.

In the 1980s, we revisited the privacy principles to test their viability given technological and social changes that had occurred and to think through the new challenges presented by these changes.

Let me take a moment to share with you our privacy principles relative to employee personnel information. They are as follows:

- * Collect, use and retain only personal information that is required for business or legal reasons.
- * Provide employees with a means of ensuring that their personal information in IBM personnel records is correct.
- * Limit the internal availability of personal information about others to those with a business need to know
- * Release personal information outside IBM only with employee approval, except to verify employment or to satisfy legitimate investigatory or legal needs.

These principles apply to all personal information but have particular meaning for medical information which, I believe, deserves the greatest degree of protection. In IBM, access to confidential medical records is limited to IBM medical staff and department personnel under their immediate supervision. They will provide access only:

- * to benefits plan administrators who may review information needed for determining eligibility for benefits
- * to others with a need-to-know to evaluate medical recommendations, medical restrictions and accommodations as they relate to the work environment and ability to perform the job

- * to legal counsel when medical status or information is at issue or required.

All employees may obtain copies of their records from the IBM medical department. Further, with few exceptions, we require our medical staffs to obtain prior approval of the employee before either disclosing or seeking confidential medical information.

Because we believe that empowered employees with knowledge of their rights is our best assurance that these rules will be followed, we publish our principles and guidelines in our About Your Company booklet which is available electronically to all employees.

We provide written guidelines for adhering to IBM's policies on privacy as they pertain to the handling of confidential medical information in our medical manual which is unclassified and available to anyone for review. I am providing this committee with copies of this material.

In addition to the information which is contained in our own internally generated medical records, we recognize the need to protect employee medical information associated with our benefits programs. IBM provides a wide array of benefits to our employees, many of which involve treatment for medical conditions. Consistent with our emphasis on employee privacy, we have placed restrictions on our benefits contract administrators on how this information can be used and even what information they will pass on to us. For example, our plan administrators receive only aggregate data derived from the medical records available to the carriers which does not permit linkage of any individual employee with a particular medical condition.

We have imposed these restrictions because we believed it was important to strike the right balance between the needs of the business and the need to protect an employee's privacy. The fact that we have been able to continue to provide our employees a broad array of medical benefits at reasonable costs while operating with these self-imposed restrictions is proof that maintaining high standards of confidentiality need not compromise efficiency.

We believe the objectives of H.R. 4077 are well-grounded. They fundamentally agree with our own company's privacy principles and practices. They strive to create a balance of purpose. The general responsibilities outlined in your bill for health information trustees are consistent with the responsibilities we have placed on ourselves at IBM.

Specific Comments on H.R. 4077

Mr. Chairman, you have embarked upon a difficult but very important challenge, and we look forward to continuing our work with you and your staff. I would like to now narrow our comments to the particulars of the legislation.

As we have said, H.R. 4077 is consistent with IBM's own privacy principles and our call for uniform federal guidelines in health care. The fundamental, flexible approach taken by the bill should enable parties to meet those guidelines. It should also encourage organizations to develop innovative approaches in order to meet their compliance obligations. Furthermore, this flexibility should greatly minimize cost.

The concept of a health information trustee, we believe, is a good one and preferable to the concept of an owner of health-related information. We believe questions of ownership are less tractable, and ultimately less relevant, than those of access.

We do think some clarification would be helpful relevant to the definition of "relating to the provision of and payment for health care." As we indicated, many companies engage employees and providers in discussions to prompt proper and expedient care and return to work. We generally do not consider that being a provision of care.

Affiliated with this is a concern we have over judgments employers must make regarding an employee's ability to perform a job or continue to be eligible for paid or unpaid leave according to company policy. While this is not specifically included in the language of your bill, it is addressed in your executive summary questions and answers on page 5, question 13. The relevant answer states "use of information about employees for purposes unrelated to treatment or payment will not be permitted."

We would ask that you help us find a way to pursue your objectives while addressing the particular needs of the employers in this case.

Let me also note for the committee that an employer's obligations under the Occupational Safety and Health Act (OSHA) require the submission of information to "OSHA logs." These logs are publicly available information with open right-of-access to anyone. They contain personal identifiers and, increasingly, diagnostic information. Our question would be, "Is this 'protected health information' and, if so, how are the trustee obligations of safeguarding privacy to be met?"

The bill also provides patients with a right-to-receive notification of disclosures of health information. This can be problematic when a request for a medical record arises well after an individual ceases to be an active employee and whose whereabouts are unknown. Perhaps some kind of transition mechanism can be developed to address this situation.

Relative to sections 114 and 115, regarding accounting for disclosures and security obligations imposed on health information trustees, we believe this is an area where information systems available today can actually enhance an organization's compliance and, most importantly, the confidentiality of an individual's medical information. Audit trails on how information has been assembled and and by whom it has been accessed are more readily available in an electronic format than a paper one.

This raises a suggestion we would like to offer affecting section 153 in subtitle D, Standards for Electronic Documents and Communications. IBM believes the general private sector standard setting process is the most appropriate forum for standards to be developed. In the area of health care-related standards, the government does have a very reasonable interest in their outcome. In fact, we feel it can play a constructive role in encouraging the acceleration of standards, especially in the clinical information systems area. However, we don't believe the government should set the standard. We would encourage the committee to modify the wording on page 64, line 5, from:

". . . shall promulgate standards . . ."

to

"shall establish standards in consultations with appropriate private sector standards organizations."

This change would be consistent with other health care reform legislation dealing with administrative simplification, in particular H.R. 3137 introduced by Representatives Sawyer and Hobson.

Finally, let me commend you for your inclusion of section 163 in subtitle E dealing with alternative dispute resolutions. We support alternatives to costly and time consuming litigation, especially ones that give both sides a fair and timely way to resolve differences.

Conclusion

Mr. Chairman, we appreciate having been given the opportunity to offer our views on the general issue of health information privacy and H.R. 4077 specifically.

We are an information technology producer and a heavy user of our own technology. We believe that our experience shows that information technology, with its ability to control information flow and access to data, can enhance the maintenance of confidentiality. It is our hope that what IBM has learned as an employer and as an information technology company can help the nation develop policies which will further the cause of health reform and assure our citizens that the confidentiality of their medical records will be maintained.

IBM is committed to enacting health care reform this year. Your legislation makes an important and valuable contribution to the reform effort. We welcome the opportunity to work with you and others in the months ahead.

EMPLOYEE MEDICAL RECORDS

1. PURPOSE: To provide guidelines for adhering to IBM's policies on privacy as they pertain to the handling of confidential medical information
2. PRACTICE:
 - a. The IBM medical departments adhere to ethical, legal and confidential standards in the handling of medical information and records including computerized medical records of employees
 - b. Medical records are confidential and private
 - c. All individual medical information except first-aid visits is to be maintained in one medical record. First-aid visits are recorded on first-aid cards or electronic files
 - d. Prior approval of the employee (releases) will be obtained before either disclosing or seeking confidential medical information except in:
 - (1) A medical emergency
 - (2) Where such disclosure is required by law
 - (3) Where the employee's medical condition is an issue between the employee and the company
 - e. Unsolicited medical information regarding employees received by management or personnel is to be forwarded to the medical department
 - f. Access to confidential medical records is limited to the IBM medical department staff
 - g. Neither management nor personnel may request an employee's medical record nor contact nor consult with an employee's private physician
3. PROCEDURE:
 - a. Employee's medical record: A medical record for each employee is maintained in a separate folder. The medical record tab is to contain the employee's identification number, last name, and initials:
 - (1) Medical Record Folder ZM04-7716 is the standard folder used for filing individual employee medical record information (see Forms Manual)
 - (2) Medical records are filed in identification number sequence by the second digit of the employee identification number
 - (3) Optional color coding:
 - (a) Color coding shall be employed by using the second, third, and fourth digits of the employee's serial number

- (b) Medical Record Folder ZM04-7716 is used with an extender tab (see Forms Manual)
- (c) If color coding has been completed in other than the standard manner, the employee medical record must be placed in the standard folder ZM04-7716 for mailing to other locations
- (4) The medical records of medical department personnel/immediate family members are to be kept in a separate file to which only medical management in another IBM medical department has access. Medical problems should be managed by the medical department that has the medical record
- (5) Forms used to maintain medical records must be approved by U.S. health and safety:
 - (a) Legal approval is required before forms are used that become part of the medical record
 - (b) All approved forms, instructions, and information on ordering are in the Forms Manual
- (6) The sequence of the medical record is chronological as follows:
 - (a) Medical Summary Information Sheet (first page)
 - (b) Medical History Sheet
 - (c) X-ray reports
 - (d) Pulmonary function tracings/results
 - (e) Laboratory reports
 - (f) ECG tracings/reports
 - (g) Supplementary records:
 - 1) Ten-day medical certificates
 - 2) Return to Work and Medical Status reports
 - 3) Worker's Compensation reports
 - 4) Miscellaneous, e.g., environmental chamber clearance, blood pressure records, radiation exposure forms, chemical profiles, etc.
 - (h) Visual records (including visual screening tests, laser exams, and tonometry tests)
 - (i) Audiometric records

- (j) Medical examinations:
 - 1) Periodic and international assignments
 - 2) Occupational History sheet
 - 3) Employment examinations
 - (k) Immunization record
 - (l) Dependent examinations for international assignments
 - (m) Voluntary Health Assessment (most recent on top):
 - 1) Computer answer sheet
 - 2) VHA data sheet
 - 3) Risk profile summary
 - 4) Laboratory report
 - 5) ECG tracings and reports
 - 6) Other VHA data, e.g., X-ray report when done
 - (n) Correspondence, third party letters, appropriate medical releases attached
- b. Medical Record Review/Coding: Each medical record should be reviewed after any medical activity:
- (1) Significant medical conditions and permanent work restrictions are coded in accordance with the guidelines in Index B6-02 and entered onto the medical system. After any data change, a new Medical Summary Information sheet (MSI) is generated locally and filed in the medical chart
 - (2) Temporary work restrictions are recorded on the Medical History sheet
 - (3) The Medical Status and Summary Report (MSSR) (see Forms Manual) is used to advise the employee and management of:
 - (a) Permanent work restrictions
 - (b) Temporary work restrictions
 - (4) Medical Records Activity listing: Each record is to be handled as indicated on the monthly activity listing sent from Sterling Forest:
 - (a) Deletions are to be sent to the new medical department within two weeks:
 - 1) Medical record
 - 2) X-rays

f. Corrections - medical data:

- (1) When an employee (or his/her designee) questions the accuracy or reliability of data contained in their record or misuse of any medical data, the medical record must be reviewed
- (2) When erroneous material is found, IBM medical records are not to be purged. Incorrect items are left intact; however, the error must be noted and a correction statement recorded on the appropriate file
- (3) If it is determined that information obtained from a third party about an employee is erroneous or allegedly erroneous then IBM will make corrections and amendments provided that the third party documents the inaccuracy. IBM will also provide the individual with the opportunity to present supplemental information for inclusion in the medical record, provided that the source of the supplemental information is also included in the record, in an effort to highlight incorrect or incomplete information
- (4) When no errors are found:
 - (a) The employee will be so informed and given the reasons for IBM position
 - (b) When appropriate, further review will be provided through the IBM medical organization or outside consultants
 - (c) The employee must be permitted to file a statement of the reason for disagreement and such statements must be carried in any subsequent disclosure of the information
 - (d) IBM medical department will include in the medical record a statement of the reason for the refusal to correct
- (5) When a correction or a notation of dispute is made and a statement of disagreement is taken, it is required that the correction, amendment, or statement of disagreement be furnished to any person specifically designated by the individual to whom we have previously disclosed the inaccurate, incomplete, or disputed information

g. Medical information:

- (1) Required by IBM - Employees are required to provide medical information to IBM medical departments when the company has a need for such information in order to carry out its policies regarding job assignments, benefits, absenteeism, international assignments, security, safety, worker's compensation, etc.
- (2) Identifiable medical information about an employee obtained for business purposes cannot be used or made available for other purposes without the individual's consent except as required by law such as OSHA 29CPR 1910.20 (see reference manual)
- (3) Where confidential medical advice is sought and there is no work performance impact and the law permits, medical is not obligated to notify management that the employee has a medical condition
- (4) Employee work restrictions both permanent and temporary will be provided to managers, personnel, and employees using the Medical Summary and Status Report form (MSSR)
- (5) The IBM medical department must be sensitive concerning handling confidential medical information about non-IBM individuals:
 - (a) The IBM medical department may require certain medical information concerning the employee's family members involved in international assignments so that administrative recommendations can be made to management:
 - 1) It is the responsibility of the employee and his or her family members to provide the required information to the IBM medical department
 - 2) Medical departments must ensure that medical information regarding an adult nonemployee and certain information concerning minors be restricted to the individuals concerned
 - (b) As outlined under the international assignment transfer instructions, an employee and family members (of legal age) may individually be given medical summaries of their individual medical status (see Index B1-07)

- (6) Personal physician contact:
- (a) The Employee Authorization for Release of Medical Information to IBM form must be utilized when there is a need to contact an employee's personal physician (see Forms Manual)
 - (b) The 10-Day Medical Certificate is to be transmitted directly from the employee or their personal physician to the medical department (see Forms Manual)
 - (c) Unsolicited information from an employee's personal physician should be used with discretion within IBM:
 - 1) It is presumed that the sender has been given permission to release this information and that he/she may be questioned by IBM for clarification of the information received
 - 2) Situations wherein the personal physician may also be an IBM contract physician require additional sensitivity
 - (d) When managers require verification of facts related to cases with medical implications, (i.e., verifying private clinic or physician visits, etc.) they should request that the employee have the appropriate information sent to the medical department for interpretation, managers should:
 - 1) Recognize that IBM standards concerning confidentiality may result in delay in the resolution of some problems
 - 2) The employee should be informed by management as to the reason for requesting the information
- h. Release of medical information by IBM medical department:
- (1) An Employee Authorization for Release of Medical Information by IBM form is required before confidential information is released (see Forms Manual):

- (a) To third parties
 - (b) Insurance companies (including IBM's own carriers, with the exception of the Worker's Compensation carrier)
- (2) An authorization for release is not required in certain circumstances:
- (a) Any section of an employee's medical file pertinent to a worker's compensation issue may be given to the IBM's worker's compensation insurance carrier. If there is any question related to pertinent information, IBM legal counsel should be sought
 - (b) Handicapped or veterans programs: For certain government programs regarding the handicapped, veterans, or others, the law may require the release of data to appropriate IBM personnel or governmental agencies. If individual identification is requested, IBM legal counsel should be contacted for advice and counsel
 - (c) Medical Disability Income Plan (MDIP):
 - 1) The administration of the MDIP necessitates divulging limited, confidential medical information to the IBM MDI Panel
 - 2) Medical confidentiality is maintained through the final levels of decision-making at which time an IBM physician is available to release and interpret only that confidential material necessary for a decision
 - (d) Second injury: In some states the law allows the insurance carrier to request an IBM employee's medical folder in an effort to establish the presence of a second injury. A release need not be obtained from the employee in these situations. Consultation with IBM legal counsel is appropriate
 - (e) NIOSH, OSHA, or other public health and regulatory agencies:

- 1) May have a legal right to confidential material with group or at times individual identification
 - 2) Under certain conditions these agencies may have a legal right to request such information
 - 3) Medical departments should advise their U.S. medical director of any such requests
 - 4) Medical departments should ask IBM legal counsel for clarification of legal requirements (see Reference Manual for Access to Employee Exposure and Medical record 29 CFR Part 1910)
- (3) International assignments medical records: As outlined in Index B1-07, under the international assignment transfer instructions, an employee and family members (of legal age) may be given medical summaries of their own, individual status
- (4) Voluntary Health Assessment--printouts: Employees requesting a copy of their VHA printout will be provided with one .
- (5) Medical personnel/management review meetings: IBM health professionals should not release confidential medical information during meetings with management and/or personnel without the prior consent of the employee
- (6) Hazardous or complex situations and cases: There are situations where physical or emotional health problems (e.g., diabetics, epileptics or severely disabled employees) require special steps to be taken to protect the individual, coworkers and the company
- (a) The employee should be advised that the medical department will release a minimum amount of medical information so that appropriate instruction can be given to managers or first-aid teams for assisting the employee in an emergency situation
 - (b) The medical confidentiality aspect of the IBM programs regarding drug and alcohol abuse should be explained to affected applicants and employees (see Indexes B3-01 and B3-02 regarding alcohol and drug abuse)

- i. Some legal requirements pertaining to medical records:
 - (1) Most state laws provide that a physician or nurse shall not disclose confidential information concerning their patient unless the patient has waived their privilege:
 - (a) By instituting a personal injury action in which the person's physical or mental condition is affirmatively put in issue, the person bringing the action may waive the privilege they might otherwise have had relative to the physical or mental condition
 - (b) Where the employee has made their medical condition an issue in a complaint (claim) an IBM attorney, or an attorney retained by IBM, or by IBM's insurance carrier, or the court's attorney, is privileged to review IBM employee medical records without a release of medical information from the employee:
 - 1) Medical information to be disclosed would involve only that medical data pertinent to the complaint
 - 2) IBM medical personnel should review the medical file with the appropriate IBM attorney in order to determine what is pertinent and what materials will be made available to other attorney(s)
 - 3) Documentation from the IBM legal department on what materials will be made available should be obtained and filed in the medical record
 - 4) IBM has an obligation not to disclose confidential information in the IBM medical record except when required by law or if there is an overriding public health consideration
 - 5) IBM, the employer, is entitled to counsel about the medical fitness of individuals in relation to work but is not entitled to diagnosis or details of a specific nature
- j. Use of tape records: Tape recorders or other similar recording devices are not to be used in IBM medical departments to record interviews with employees, managers, health professionals, or others. Any exception to this rule requires the prior clearance from the corporate director of health and safety

EMPLOYEE ACCESS TO MEDICAL RECORDS

1. PURPOSE: To provide guidelines for adhering to IBM's policies, assure compliance with legal requirements, and assure equal treatment of IBM employees (or former employees) regarding access to medical records
2. PRACTICE:
 - a. Employees are notified of OSHA access to medical records rules under 29 CFR 1910.20 by bulletin board notice. Generally, all employees are allowed access to their medical records although all employees may not be strictly covered by the OSHA access rules (see 3.F.(1) and 3.A.(4))
 - b. IBM medical personnel should be familiar with OSHA regulations and should consult with site legal or IBM US medical regarding definition of medical records, or questions related to exposure, potential harm, administrative matters or state and local laws
 - c. "Employee medical record" means a record concerning the health status of an employee which is made or maintained by an IBM medical department or IBM designated physician, nurse, or other health care provider. Employee medical record includes:
 - (1) Medical and employment questionnaires or histories (including description of the job as it relates to the medical condition and occupational exposures)
 - (2) The results of medical examinations (pre-employment, pre-assignment, periodic, or episodic) and laboratory tests (including X-ray examinations and all biological monitoring)
 - (3) Medical opinions, diagnoses, progress notes, and recommendations
 - (4) Descriptions of treatments and prescriptions
 - (5) Employee medical complaints
 - (6) Third party medical information

Employee medical record does not include:

- (1) Records concerning health insurance claims if maintained separately from the employer's medical program and its records, and not accessible to the employer by employee name or other direct personal identifier (e.g., social security number, payroll number, etc.), or
- (2) Records concerning voluntary employee assistance programs (alcohol, drug abuse, or personal counseling programs) if maintained separately from the employer's medical program and its records

- (3) Non-medical information contained in the medical record; i.e., information that does not relate specifically to the health status of the individual can be redacted after consultation with legal.
 - d. The medical department is made aware that an employee is requesting access to his/her medical record in the following ways:
 - (1) Written or oral request by the employee
 - (2) Notification by the employee's manager
 - (3) Written request by the employee's attorney, designated representative, or personal physician
 - (4) Other legal documents such as a subpoena or court order
3. PROCESS:
- a. Appropriate IBM legal advice should be obtained as necessary
 - b. The medical record is all of the information that relates to the health status of the employee (refer to 2.c. above)
 - c. Unless otherwise required by law (see section g) the medical staff shall within 15 working days of the date of the request:
 - (1) Review the record with the employee. However, if the employee does not want to review the medical record with the health care professional he or she is not required to do so
 - (2) Offer the employee a copy of the entire or portion of the medical record
 - d. Employee written or oral request to review the medical record or receive a copy of the medical record:
 - (1) Ask the employee to complete the Employee Records Request form (see Forms Manual)
 - (2) Make an appointment for the employee to see a physician or the managing nurse to review the medical record and/or receive copies of the requested portion of the medical record.
 - (3) File the medical department copy of the Employee Records Request Form in the employee's medical chart
 - (4) Complete the Medical Record Request Log assigning each entry a consecutive case number (see Forms Manual)

- e. Notification of employee's request to review their medical record by the employee's manager:
- (1) Ask the manager to initiate the Employee Records Request Form
 - (2) Make an appointment for the employee to see a physician or the managing nurse to review the medical record and/or receive copies of their medical record
 - (3) File the medical department copy of the Employee Records Request Form in the employee's record
 - (4) Log the transaction on the Medical Record Request Log
- f. Written request from the employee to release medical records to their attorney, designated representative, or personal physician:
- (1) Medical information will be released to a designated representative other than the employee's attorney or personal physician only when required by law. Consult as appropriate with legal and IBM medical directors.
 - (2) The request must be accompanied by a signed, witnessed Release of Information form from the employee (see forms manual)
 - (3) Copy the medical record or portion of the medical record requested and mail the copy to the designated address by registered mail return receipt requested
 - (4) Maintain a copy of the Release of Information form in the employee's medical record and when the return receipt is received, file it in the employee's medical record
 - (5) Make the appropriate entry on the Medical Record Request Log
- g. Legal document requiring production of an employee's medical record (such as subpoena or other legal document):
- (1) Consult with IBM legal regarding the appropriate method of response and possible notification of the employee. The legal department has the responsibility to respond to medical department requests to review subpoenas and evaluate medical records and to determine from a legal point of view how and with what information the medical department will respond to subpoenas.
 - (2) Copy the requested portions of the medical record
 - (3) Mail to the designated address by registered mail and return receipt requested

- (4) File a copy of the legal document in employee's chart as well as the return receipt
 - (5) Make the appropriate entry on the Medical Records Request Log
 - (6) Consult as appropriate with your managing physician or IBM US medical directors
- h. Managing information that could be harmful to the employee, co-worker, or family member:
- (1) Consult with IBM legal regarding the appropriate method of response.
 - (2) Copy the requested portion of the medical record, redacting the harmful information before giving it to the employee
 - (3) Inform the employee that information has been redacted
 - (4) If the employee still requests the information which you have redacted and you have serious concerns for safety or well being, immediately consult with IBM legal and your IBM US medical director. Information will only be released if required by law
 - (5) If the information is required by law to be released, obtain a signed, witnessed release of information form from the employee to release the information to their designated representative (usually their attorney or private physician)
 - (6) This should be done even with the knowledge that the employee's representative may release the information to the employee
- i. Handling third party medical information (ref. 2.C.(6))
- (1) New release forms (ZM04-8086 revision level 7 and above) for third party information will alert outsiders to IBM's policy on access to medical records; therefore material submitted in response to this form may be released to employees or their designated representative
 - (2) In the case of material received pursuant to old releases, (ZM04-8086 up to and including revision level 6) the information should be withheld unless it is required by law to provide it. Legal advice should be obtained in this situation
 - (3) Drug and alcohol information labeled under 42 CFR, part 2, is confidential and may not be released to outside third parties unless proper releases (ZM04-8106) are completed by the employee

ACCESS TO EMPLOYEE EXPOSURE AND MEDICAL RECORDS

In accordance with Occupational Safety and Health Administration regulation 29 CFR 1910.20, employees exposed to toxic substances such as those listed in the NIOSH Registry of Toxic Effects of Chemical Substances, or to harmful physical agents such as extreme noise, vibrations, etc., may have access to their company-maintained exposure and medical records.

IBM has a comprehensive health and safety program and our health and safety record reflects a continuing commitment to the well being of all employees. An ongoing monitoring program is in effect for all work areas with potential operator exposures to harmful substances or physical agents. The industrial hygiene or medical department maintains copies of the employee exposure records required by 29 CFR 1910.20, and you can contact your manager to obtain copies of your records.

The IBM medical department is responsible for maintaining employee medical records and shall, upon request, provide information from or copies of medical records, and will be able to answer any questions you might have regarding this regulation.

The medical/safety department will make readily available to you a copy of 29 CFR 1910.20 and its appendices.

Mr. CONDIT. Mr. Bolan.

STATEMENT OF ROBERT S. BOLAN, CHAIRMAN, MEDIC ALERT FOUNDATION INTERNATIONAL, TURLOCK, CA

Mr. BOLAN. Mr. Chairman and members of the subcommittee, I am Robert Bolan, vice chairman of the board of directors of Medic Alert Foundation United States in which I serve as a volunteer. And I am the full-time employee of a medical specialty society serving as executive director, so I am sort of both on the patient and provider side of health information at the same time.

With me today seated in the audience is Dr. Richard Wilbur, who is president and CEO of Medic Alert Foundation, United States and Medic Alert International.

On behalf of Medic Alert, I am pleased to testify today on the Fair Health Information Practices Act of 1994. Medic Alert strongly supports a uniform national bill for privacy protection.

We appreciate H.R. 4077 and urge rapid work and passage. The issue of personal health information is one in which Medic Alert has intimate knowledge. It has been our mission to use such information to protect and save lives for nearly 40 years.

Medic Alert Foundation United States is a nonprofit medical information service established in 1956. The Medic Alert emblem represents an internationally recognized emergency information network providing critical patient information anywhere in the world, 24 hours a day.

Medic Alert protection is a recommended part of the preventative health care plan for the estimated 25 percent of Americans with hidden medical conditions such as hypertension, heart conditions, medication allergies, diabetes or any one of 200 other conditions which could seriously affect diagnosis and treatment in a medical emergency.

In addition, the Medic Alert system serves to maintain records if the patient desires such, as with advanced directives, and there was some recent research published indicating that advance directives can save approximately two-thirds of the cost of care, in many instances.

Medic Alert speaks for 2.4 million members in the United States and 4 million members worldwide when they are disoriented, unconscious, too young or otherwise unable to explain their medical conditions. Medic Alert service starts with a neck or wrist emblem, custom engraved with summarized critical medical facts and a 24-hour telephone hot line number enabling emergency responders to begin treatment immediately.

By accessing Medic Alert's emergency line, first responders receive vital details from the member's computerized record, including conditions, medications, allergies, physician, pharmacy, family contacts, information that has helped avoid life-threatening complications and even death. The key to most of Medic Alert's medical information service is that patients act in their own interest to request that the information be held and used by Medic Alert.

Medic Alert has always been highly protective of the privacy and confidentiality of patient information. Our U.S. information data base of 2.4 million patient records is closed to outside business in-

terests and exists solely in direct relationship with and solely for the benefit of the private citizen patient.

The sole purpose of this data base is to provide emergency information about individuals to qualified health professionals and first responders to aid in emergency treatment or to locate the patient's physician or family. Members names are not engraved on our emblems. Information is only accessed by using member identification numbers.

These identification numbers are unique. They are not social security numbers and are neither publicized nor released to those outside of Medic Alert. The collect-call emergency response center phone number is published on Medic Alert emblems for emergency use only.

Callers are required to submit their name, title, facility, and phone numbers for verification purposes and if in doubt, emergency response center personnel verify a callers identity prior to releasing confidential medical data.

Medic Alert supports legislation on privacy and confidentiality that puts severe restrictions on the type and amount of medical information that is available by online data transmission or otherwise to anyone other than qualified medical personnel and then only with full disclosure to and consent of the patient.

We support legislation that allows an individual to govern the manner in which his or her private information is maintained, transmitted or otherwise handled. Medic Alert advocates the use of private nonprofit nongovernmental services designed in the best interest of the individual for the maintenance of private medical information.

As an example of patients' keen interest in how their medical information is maintained, approximately 10,000 patients of Medic Alert's data base have requested that one or more of their medical conditions not be engraved on their emblem nor listed in their wallet cards. Conditions such as Alzheimers disease and epilepsy are perceived by these patients to carry a social stigma, perhaps causing employment difficulties, and as a result they request that body worn or carried identification not associate them with their condition.

These patients have, however, authorized the release of their medical conditions to medical personnel in an emergency. Under this authorization, Medic Alert releases patients' medical information following the established confidentiality protocol.

I would like to comment briefly—there is more in our written statement—on our relationship with the Shiley heart valve program. The confidential medical information on Medic Alert's data base is not only patient authorized but patient disclosed.

Only in the case of Medic Alert's heart valve program is that information not always obtained directly from the patient. Medic Alert Foundation U.S. operates under a grant from Shiley Inc., of Irvine, CA, to locate and contact approximately 33,000 patients who received implanted 60- and 70-degree Bjork-Shiley Convexo-Concave mechanical heart valves in the United States and Canada.

The purpose of Shiley's program with Medic Alert is to be able to provide important information to patients should the need arise. Patient-specific information including addresses and implant device

information, social security number, date of birth and names and addresses of physicians and surgeons are retrieved from several sources. The protocol is described in the testimony.

A majority of contacted Shiley heart valve recipients have chosen to become members of Medic Alert's ID service once they learned about the service. Medical information is only exchanged between the heart valve program and Medic Alert's data base upon authorization by the patient, but there is an exchange of information between the two subdata bases.

Because of our experience in assisting emergency medical care, Medic Alert offers the following issues for your consideration: First, the release of personal medical information should be treated differently in emergency situations. And you have done that in section 126 of H.R. 4077.

We encourage the insertion of a clause into that section to protect individuals who, acting in an emergency in good faith and in accordance with a patient's expressed desires, releases personal medical information.

Second, as an organization with worldwide membership and U.S. members who travel abroad, we also encourage the inclusion of section 152(b)(2) permitting access to protected medical information outside of the United States to alleviate emergency circumstances. While we support the protection of private medical information, we encourage the subcommittee to exempt emergency circumstances from the restrictions provided in section 152. Americans traveling abroad can only be assured Medic Alert protection if emergency responders are able to access information from Medic Alert's USA data base.

In conclusion, Medic Alert is currently the largest information data bank of patient-supplied medical information in the world. Medic Alert employs about 150 individuals in Turlock, CA. It has been estimated that Medic Alert helped avert tragedy in over 200,000 medical emergencies since the foundation's inception.

Speed of delivery is crucial for emergency treatment. The emergency room or trauma scene is a diagnostic epicenter where lives are won or lost by seconds. Emergency physicians and paramedics walk a tightrope between protecting a patient's right to privacy and accessing private medical information when he or she is unable to authorize disclosure.

Medic Alert has grappled with this privacy issue since 1956. When in doubt, we will always err on the side of saving a life.

On behalf of Medic Alert, I would like to thank you for the opportunity to address this multifaceted issue. Establishing fair practices with regard to private medical information will help protect consumers, who are also our members.

We look forward to serving as a resource as this legislation is integrated into overall health care reform, and we appreciate your initiative in introducing and pursuing the legislation. We believe it should be enacted promptly.

Mr. CONDIT. We appreciate your participation and we appreciate, Dr. Wilbur for being here today as well.

[The prepared statement of Mr. Bolan follows:]



STATEMENT OF ROBERT BOLAN, PhD
VICE CHAIRMAN OF THE BOARD OF DIRECTORS

MEDIC ALERT FOUNDATION U.S.

TO
THE UNITED STATES
HOUSE OF REPRESENTATIVES

**INFORMATION, JUSTICE, TRANSPORTATION AND AGRICULTURE
SUBCOMMITTEE
OF THE
COMMITTEE ON GOVERNMENT OPERATIONS**

MAY 4, 1994

INTRODUCTION

Mr. Chairman and Members of the Subcommittee, I am Robert Bolan, Vice Chairman of the Board of Directors of Medic Alert Foundation United States. With me today is Richard Wilbur, MD, JD, who is President and CEO of Medic Alert Foundation U.S. and Medic Alert Foundation International. On behalf of Medic Alert, I am pleased to testify today on the Fair Health Information Practices Act of 1994. Medic Alert strongly supports a uniform national bill for privacy protection. The issue of personal health information is one in which Medic Alert has intimate knowledge. It has been our mission to use such information to protect and save lives for nearly 40 years.

Medic Alert Foundation U.S. is a nonprofit medical identification service established in 1956. The Medic Alert emblem represents an internationally recognized emergency information network providing critical patient information anywhere in the world, 24 hours a day. Medic Alert protection is a recommended part of the preventative healthcare plan for the estimated 25% of Americans with hidden medical conditions such as hypertension, heart conditions, medication allergies, diabetes or one of 200 other conditions which could seriously affect diagnosis and treatment in an emergency. Medic Alert speaks for 2.4 million members in the U.S. and 4 million members worldwide when they are disoriented, unconscious, too young, or otherwise unable to explain their medical conditions.

Medic Alert's service starts with a neck or wrist emblem custom engraved with summarized critical medical facts and a 24-hour telephone hot line number, enabling emergency responders to begin treatment immediately. By accessing Medic Alert's emergency line, first responders receive vital details from the member's computerized record including conditions, medications, allergies, physician, pharmacy and family contacts --

information that has helped avoid life threatening complications and even death. Wallet cards are also supplied which augment the engraved emblem with additional information such as individuals to contact and medications.

Confidentiality of Medical Information

Medic Alert has always been highly protective of the privacy and confidentiality of patient information. Our U.S. information database of more than 2 million patient records is closed to outside business interests and exists solely through the direct relationship with, and solely for the benefit of, the private citizen-patient. The sole purpose of this database is to provide emergency information about individuals to qualified health professionals and first responders to aid in emergency treatment or to locate the patient's physician or family. Members' names are not engraved on our emblems; information is only accessed by using member identification numbers. These identification numbers are unique and are neither publicized nor released to those outside of Medic Alert. The collect-call Emergency Response Center phone number is published on Medic Alert emblems for emergency use only. Callers are required to submit their name, title, facility and phone number for verification purposes, and if in doubt, Emergency Response Center personnel verify a caller's identity prior to releasing confidential medical data. As expanding technology enables us to increase the speed by which we transmit data, we strive to incorporate safeguards to protect sensitive patient information. We are building special confidentiality safeguards into our new faxing program prior to transmitting medical data electronically in emergencies. Our new physician notification program encourages physicians to verify the accuracy of their patients' medical information held on our database system. In summary, the Board of Directors and staff of Medic Alert pledge to uphold a bond with its membership that assures privacy and confidentiality in the operation of its central patient-record database.

Medic Alert supports legislation on privacy and confidentiality that puts severe restrictions on the amount and type of personal medical information that is available, by on-line data transmission or otherwise, to anyone other than qualified medical personnel and

then only with full disclosure to, and consent of, the patient. We support legislation that allows an individual to govern the manner in which his or her private information is maintained, transmitted, or otherwise handled. We further support legislation that protects professional medical personnel from data exploitation by other parties.

Medic Alert advocates the use of private, non-profit, non-governmental services, designed in the best interests of the individual for the maintenance of private medical information. The private citizen's personal medical information should not be public knowledge.

Special Circumstances

Approximately 10,000 patients on Medic Alert's database have requested that one or more of their medical conditions not be engraved on their emblem nor listed on their wallet card. Conditions such as Alzheimers disease and epilepsy are perceived by these patients to carry a social stigma and as a result they request that body-worn or carried identification not associate them with their condition. These patients have however, authorized the release of their medical conditions to medical personnel in an emergency. Under this authorization, Medic Alert releases patients' medical information following the established confidentiality protocol.

Shiley Heart Valve Program

The confidential medical information on Medic Alert's database is not only patient-authorized, but patient-disclosed. Only in the case of Medic Alert's Heart Valve Program (HVP), is that information not always obtained directly from the patient.

Medic Alert Foundation U.S. operates under a grant from Shiley Inc., Irvine, California, to locate and contact an estimated 32,933 patients who received implanted 60 and 70 degree Bjork-Shiley Convexo-Concave mechanical heart valves in the U.S. and Canada.

The purpose of Shiley's program with Medic Alert is to be able to provide important information to patients should the need arise. Patient-specific information, including addresses, implant device information, social security number, date of birth, and names and addresses of physicians and surgeons are retrieved from several sources. These sources include Shiley implant cards, hospital, surgeon or physician research reports, the list of individuals who responded to the Bowling class action settlement notice, and from patients themselves.

The implanting surgeon or treating physician is contacted first under a protocol agreed upon by Shiley and the Food and Drug Administration in 1991. Once a patient has been located, Medic Alert's Heart Valve Program (HVP) staff communicate directly with the patient by phone or mail. Update letters are sent which advise the patient of current information on file and request the patient to correct or provide information needed; thereby patients are apprised of all information in their files. However, if a physician informs Medic Alert's HVP staff not to communicate with the patient, all communications are sent directly to the physician for as long as the patient is believed to be living. Patient communication is handled similarly when it is confirmed that a physician's office is tracking an implanted patient. If contact cannot be made through a physician, the database services of TRW, EQUIFAX and the mail forwarding services of the Social Security Administration have been used. For patients with known social security numbers, the National Death Index and Social Security Administration Death Master File have been used to determine if the patient is still living.

A majority of contacted Shiley heart valve recipients have chosen to become members of Medic Alert's ID service. Medical information is only exchanged between the HVP Program and Medic Alert's database upon authorization from the patient.

Discreet medical information is held strictly confidential and secured on a computerized database with safeguards to protect patient identity. Patient identity is never released to outside parties; Shiley is only provided with identification numbers and valve

numbers. Patient names are not released to Shiley.

Specific Concerns

Because of our experience in assisting emergency medical care, Medic Alert offers the following issues for your consideration. First, the release of personal medical information should be treated differently in emergency situations. We encourage the insertion of a clause into section 126 of HR 4077 to protect individuals who, acting in an emergency, in good faith release personal medical information into the wrong hands.

Second, as an organization with membership worldwide and U.S. members who travel abroad, we also encourage the inclusion of Section 152 (b) Exceptions (2) permitting access to protected medical information outside of the United States to alleviate emergency circumstances. While we support the protection of private medical information, we encourage the Subcommittee to exempt emergency circumstances from the restrictions provided in Section 152. Americans traveling abroad can only be assured Medic Alert protection if emergency responders are able to access information from Medic Alert's stateside database.

CONCLUSION

Medic Alert is currently the largest information data bank of patient-supplied medical information in the world. It has been estimated that Medic Alert helped avert tragedy in over 207,000 medical emergencies since the Foundation's inception. Speed of delivery is crucial for emergency treatment. The emergency room or trauma scene is a diagnostic epicenter where lives are won or lost by seconds. Emergency physicians and paramedics walk a tightrope between protecting a patient's right to privacy and accessing private medical information when he or she is unable to authorize disclosure. Medic Alert has grappled with this privacy issue since 1956 and although 100-percent confidentiality cannot be guaranteed, we will always err on the side of saving a life.

On behalf of Medic Alert, I would like to thank you for the opportunity to address this multifaceted issue. Establishing fair practices with regard to private medical information will help protect consumers, who are also our members. We look forward to serving as a resource as this legislation is integrated into overall healthcare reform. Thank you.

Mr. CONDIT. Professor Schwartz.

STATEMENT OF PAUL SCHWARTZ, ASSOCIATE PROFESSOR OF LAW, UNIVERSITY OF ARKANSAS LAW SCHOOL, FAYETTEVILLE, AR

Mr. SCHWARTZ. Thank you, Mr. Chairman and members of the committee for the opportunity to talk with you today about medical privacy. I am Paul Schwartz; I am an associate professor of law at the University of Arkansas in Fayetteville, and my area of expertise is data protection law with an emphasis on international issues.

I would like to do three things today. First, I want to first briefly describe the inadequacy of the current legal regulation of health care information. Then I would like to discuss with you some important developments in Europe.

Finally, I would like to argue that there is a need not only for Representative Condit's bill for fair information practices but passage of a bill creating a national data protection board.

I can also say that since I am from Arkansas and I am here under oath, I would be glad to answer any questions that you might have about our basketball team.

Let me begin by talking about the inadequacy of current medical data protection in the United States. I think I have some examples that I can give you that will indicate this inadequacy.

The first example are the kinds of mailing lists that are currently for sale in the United States. If you wanted to go out today you could buy a list of 5 million elderly, incontinent women. You could buy a list of 6 million allergy sufferers or 67,000 people with epilepsy.

Another example of the inadequacy of the current legal regulation of medical privacy is the fact that we now have more Federal privacy protection for the videos that we rent than for our medical records. To give you another example, the best Federal medical protection in the United States is for alcohol or drug abusers in federally funded programs. But if you are an alcohol or a drug abuser and you are not in a federally funded program, you are not going to get very good protection for your health care information. And if you are not an alcohol or drug abuser and you are not in a federally funded program, you are also not going to get very good Federal protection.

My final example that I would like to share with you of the inadequacy of the current regulation is the kind of blanket disclosures that are used to justify release of medical information. In medical law in general, we have a notion of "informed consent." Informed consent is a very important legal notion and it exists before the doctor can treat you, before he can touch your body.

Informed consent is also required before a doctor or a service payer or a hospital can do anything with your medical information. But what has happened under the current system is that instead of having informed consent, we have "blanket consent." Blanket disclosure releases are now used. Consumers sign broad blanket disclosures and these forms are used to justify the use of their data all over the map.

I would like now to talk about the kinds of Federal regulations we have and the kinds of State regulations we currently have. The problem with the Federal regulations is that they are either for information that is in Federal control and Federal hands, and then we have some constitutional protection and we have some protection under the Privacy Act, or they are for certain kinds of narrow sectors.

The problem is that most medical information is not in Federal hands, in Federal control, and most medical information is not in the kind of narrow sectors that are covered. So for example, we do have Federal medical protection for social security records and we do have it for alcohol or drug abuse patients in Federal clinics, but most medical data are not going to be covered by this Federal protection.

What happens on the State level? On the State level, we have a patchwork of laws and there are weaknesses in all of these legal approaches. But even more importantly, is there is a need now for uniform regulation. If we go from State to State, we are going to find that there is a great difference in the kind of regulation that is provided, but health data now flow from State to State and this is because we have insurers who are located in different States. For example, for the University of Arkansas in Fayetteville, our insurer is located in Memphis, TN.

Another reason why health data flow from State to State is we have HMO's and regional health care alliances located in a number of States.

Finally, we are moving to a situation where we are going to have regional health care organizations located in several States. The Clinton health bill proposes a national data network of health care information, so we are going to go from a situation where we have data flowing within a few States, to an national data network. And as a result of this interstate flow of health care information, we need a Federal response. We need that Federal response now.

When the system goes online, we need to have the protections in place and not in 3 years, not in 4 years and not in 5 years. The same way if you build a super highway, and you are going to have cars driving down it, we are not going to wait to paint the lines down the road, we are not going to put up the signs of where people can get off in 3 or 4 or 5 years. We need those protections now when the system is created.

Second, I would like to talk about some important international developments. European laws offer good protections in the area of medical privacy. There is another issue here; it is not only that the European laws do a good job in Europe, but inadequate protection of medical data in the United States can lead to the blocking of the transfer of personal data from Europe to the United States.

European protection within individual nations now takes place through data protection laws, omnibus laws that are then backed up by sectoral measures. And in general, there is a high level of protection in Europe for medical privacy.

But there are also important European-wide developments that I would like to talk to you about. The first one is an European-wide treaty, a Convention of the Council of Europe dealing with data protection law. That treaty allows European nations to block the

transfer of data from Europe to third countries, including the United States.

The critical language is if the third country does not offer "equivalent protection," the European country can block the transfer. This same approach is taken under a draft directive of the Commission of the European Union which also allows transfers to be blocked to third countries.

Moreover, if you look at national laws in Europe, they also allow transfers of data to be blocked to countries that do not have adequate protection. An example of that is in the Federal German Data Protection Laws, sections 17 and 28.

What does all this mean? There are a number of United States companies that will be affected by these kinds of provisions in European laws that allow for transfers of data to be blocked.

I would like to talk about three kinds of companies in the United States that will be affected. The first kind of corporation or company is the international corporation located in many countries throughout the world that needs to send employee records back to the United States.

Another kind of American company that would be affected by the inadequate protection of medical privacy in this country are the pharmaceutical companies. Pharmaceutical companies in the United States must now carry out international drug studies so that their products can be approved not only in the United States but throughout the world. And this research might be hampered by the inadequate protection for medical privacy in this country.

Finally, the third corporation, the third American business that can be affected by our inadequate protection for health care information, is in the information processing sector. U.S. companies now compete globally for information processing contracts and many of these contracts involve the processing of health care information.

U.S. companies will be at a competitive disadvantage unless we improve the protection for health care information within this country. It makes good business sense for the United States to institute Federal measures of data protection for health care information.

Finally, the last area that I would like to talk about is the need for a Federal board to carry out data protection oversight. I would like to add that there is such a bill now before the Senate which has been introduced by Senator Paul Simon.

The reason for independent governmental oversight is our need for institutional expertise to monitor change in technology and in data processing practices. We also need a government agency that is available to assist the legislature, the citizens and the business community in understanding the implications of these data protection practices.

I can also tell you that almost all other western countries now have such an independent data protection board. And the world's data protection commissioners now meet on a regular basis.

This discussion of international data protection concerns goes on today without substantial American involvement, and the creation of such a data protection board would increase and improve American participation in this debate.

I urge passage of Representative Condit's bill to create fair information practices for health care information, and I urge the passage of a bill to create a U.S. Data Protection Board.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Schwartz follows:]

TESTIMONY OF PAUL SCHWARTZ,
ASSOCIATE PROFESSOR OF LAW,
UNIVERSITY OF ARKANSAS SCHOOL OF LAW, FAYETTEVILLE

TO
THE GOVERNMENT INFORMATION, JUSTICE AND AGRICULTURE
SUBCOMMITTEE
OF THE
HOUSE COMMITTEE ON GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES
ONE-HUNDRED-THIRD CONGRESS

Wednesday, May 4, 1994

Mr. Chairman and members of the Committee, thank you for the opportunity to testify regarding the privacy of health care information.

I am an Associate Professor of Law at the University of Arkansas School of Law, Fayetteville. Currently, I am one of the investigators preparing a formal evaluation of American data protection law for the Commission of the European Community (Brussels).

I have published and lectured on issues concerning computers and privacy in the United States and Europe. In 1989, I was the first American to address the Annual International Meeting of Data Protection Commissioners at a conference held in the French Senate, Paris, France. My scholarship and essays have appeared in such periodicals as the Columbia Law Review, Hastings Law Journal, American Journal of Comparative Law, and the Partisan Review.

We meet today at an critical moment for a discussion of medical privacy. Public opinion polls show that Americans are deeply concerned with how their personal data are handled by the government and private companies. These polls reveal widespread alarm over threats to privacy; these concerns cut across all demographic subgroups within American society.¹ Indeed, over

¹ See Harris-Equifax, Health Information Privacy Survey 2 (1993) (eighty percent of the American population are very or somewhat concerned about threats to their personal privacy) [hereinafter cited as Health Information Privacy Survey].

three-quarters of the public currently believe that they have lost control of how personal information is circulated and applied by companies. Americans are also highly concerned about the processing of their health information.²

There are three topics I wish to discuss with you this morning. The first is the weakness of the current laws that control the application of medical information. The second topic concerns significant European developments concerning data protection law. The term "data protection" refers to the area of law that structures the application of personal information.³ Both the weaknesses of the current American approach and the developments in Europe offer strong grounds for passage of Representative Condit's bill to establish a code of fair information practices for health information (H.R. 4077).

Yet, this bill should be accompanied by passage of another law: one that establishes a national data protection board. My third topic concerns the role of such a board. A data protection agency is necessary to carry out ongoing oversight of technological developments and to advise the legislature on the extent of compliance with fair information practices. It is also needed to help citizens in the exercise of their rights and to assist the American business community in responding to national and international regulations.

² Id. at 87-103.

³ See generally David H. Flaherty, *Protecting Privacy in Surveillance Societies* (1989); Paul Schwartz, *Data Processing and Government Administration*, 43 *Hastings L.J.* 1321 (1992).

I

Protection of Medical PrivacyA. Data Processing and Medicine

The Clinton Administration has committed itself to the creation of a national program of health insurance, and any health care reform is fated to increase the computerization of medical data. Such increased reliance on computerization will be necessary to help reduce waste and fraud and to increase the efficiency of both medical practice and the payment process. It will also heighten the threat to a specific kind of privacy interest of patients, namely their right of informational self-determination. I wish now to describe the nature of information processing, first in general terms and then in the medical context, and to explain the interest in informational self-determination.

Information has become vital to the American economy. The contribution of information services to the Gross Domestic Product exceeds even that of manufacturing. The now-common term "information society" expresses the significance of this collection, coordination, and analysis of data in the United States. American business must continue to develop and exploit information technology to maintain our nation's economic well-being.

Moreover, the government, like industry, has come to rely on

the processing of personal information with the latest technology. In fact, the federal government utilizes the world's largest collection of computers.⁴ The intensity of the federal government's reliance on administration through information technology is indicated by the large number of its computers that are equipped with communication links to other government computers. The federal government leads all sectors of American industry or trade in the percentage of its computers equipped with such communication links.⁵

Information processing is now essential to business and government in the United States. It also plays a critical role in the provision, regulation and financing of medical services by government and business. Despite a past social tradition of deference to the medical profession's self-regulation, the state has seized upon the collection and application of information as a way to control doctors, regulate national health expenditures, and help doctors control patients. Thus, in application of the Medicaid program, the state collects and reviews personal data to decide whether a given patient is eligible for services defined as medically necessary.⁶ Private health plans and hospitals also collect and process personal information technology to

⁴ Office of Management and Budget, Management of the United States Government, Fiscal Year 1989, at 72 (1989).

⁵ U.S. Census Bureau, Statistical Abstract of the United States 952 (1990).

⁶ See, e.g., *Cowan v. Myers*, 232 Cal. Rptr. 299 (1986) (state and not physician decides which medical services are necessary and, therefore, subject to state funding).

strengthen administrative control. This application is particularly significant in the carrying out of utilization review under both Medicaid and Medicare. In addition to the example of utilization review, one can add diagnosis related groups and treatment protocols as examples of the ways in which medical practices are being standardized and governed with the help of information technology.

Information technology may be the last best hope to control health care in a rational way. It renders the enormous amounts of information involved in diagnosing, treating and billing patients accessible to external control. In the near future, electronic cards ("smart cards") carried by citizens may contain personal health care information. Another likely future development will be electronic patient records that are used within nation-wide electronic health care networks. This focus on the practice and regulation of medicine through the processing of personal health care information has a number of potential drawbacks, one of the most important of which is the threat to the privacy of patients.

Privacy is, of course, a concept that refers to a wide variety of interests in American law. For conceptual clarity, I wish to explain the critical privacy interest at stake here as one in "informational self-determination." The law has long recognized another aspect of self-determination in health care, namely that of informed consent. Informed consent protects a patient's interest in personal autonomy by requiring that doctors

and patients discuss relevant concerns and exchange relevant information before agreeing upon a course of medical treatment.

Informational self-determination also relates to this interest in decisionmaking by the patient. Self-determination can only exist when an individual has an underlying capacity for critical reflection. Yet, the computer creates a strong pressure for individuals to conform to digital reality. This pressure, which is dreadfully exacerbated by uncertainty as how bureaucracies are processing personal data, can have a negative effect on the human ability to make free choices. This method of administration can weaken an individual's capacity for critical reflection and participation in society.

Informational self-determination depends on the law shaping the use of medical data in the public and private spheres. The law must put fair information practices in place so patients understand the nature and structure of the processing of their personal data and be assigned a role in decisions about how their data will be used. The kinds of fair information practices that are necessary include a specification of collection purposes before personal data are sought; limitations on additional use of personal data; limitations on the collection of unnecessary data and their storage; and the data subject's ability to have access to and correct personal information. At present, the law in this country fails to require in any consistent, effective fashion that these fair information practices be in place for health care information.

B. Current Data Protection Measures

The present regulatory scheme in the United States consists of federal law that applies only to data in the control of the government or to certain, specific kinds of health data. The regulatory scheme also includes state measures that create a patchwork of insufficient protection. Moreover, the laws of the various states are far from uniform. In an age when interstate transfers of data are becoming prevalent, this lack of uniformity is itself an additional weakness in American medical data protection. At present, the best protection for any medical information in this country is provided for individuals who are enrolled in federally-financed drug and alcohol treatment centers.

The weakness of the regulation of health care information has been commented upon by many observers. In 1977, the federal Privacy Protection Study Commission noted the billions of visits that Americans make to physicians in a single year. Yet, for this blue ribbon Commission, "even more staggering is the realization of how many people besides the medical care providers who create a medical record have access to it."⁷

The legal scheme has not improved since the report of the Privacy Protection Study Commission. A recent study of the

⁷ Privacy Protection Study Commission, Personal Privacy in an Information Society 277 (1977). The Commission also noted that patients were, by and large, denied access to their records. Id.

Office of Technology Assessment concludes, "The present legal scheme does not provide consistent, comprehensive protection for privacy in health care information, whether it exists in a paper or computerized environment."⁸ According to the Committee on Regional Health Data Networks of the Institute of Medicine, "the threats and potential harms" from disclosure and redisclosure of health record information "are real and not numerically trivial."⁹ Finally, Sheri Alpert, a government policy analyst, notes, "video rental records are afforded more federal protection than are medical records."¹⁰

Enormous demand exists today for medical information. Beyond the traditional doctor-patient relationship and the provision of health services in hospitals, medical data are sought after by a wide variety of public and private organizations. Alan Westin has made a highly useful description of the flows of personal medical information in the United States today. Westin describes three zones of applications: zone one is direct patient care (doctors, clinics, hospitals, nursing homes); zone two, supporting and administrative activities (service

⁸ Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information* 13 (1993).

⁹ Committee on Regional Health Data Networks, *Institute of Medicine, Health Data in the Information Age* 156 (Molla S. Donaldson & Kathleen N. Lohr, eds. 1994) [hereinafter cited as *Institute of Medicine Study*].

¹⁰ Sheri Alpert, Smart Cards, Smarter Policy: Medical Records, Privacy and Health Care Reform, *Hastings Center Report* 13 (November-December 1993). See Joel R. Reidenberg, *Privacy in the Information Economy*, 44 *Fed. Comm. L.J.* 195, 227-34 (1992).

payers, third party administrators, quality of care reviews); zone three, broader uses of health data, termed "secondary uses," (credential and evaluation decisions, public health reporting, social welfare programs, direct marketing).¹¹ More organizations than ever before are seeking -- and obtaining -- access to health information.

The current patchwork system of data protection has been unable to impose an adequate legal structure on the enormous demands for medical data. One example of the failure of the current system of legal regulation is the abuse of the notion of "informed consent" to information disclosure. Just as respect for physical self-determination requires "informed consent" before medical treatment, informational self-determination requires "informed consent" before processing and sharing of health care information. Yet, service payers, such as insurance companies, often have their customers, the future consumers of health care services, sign broad, "blanket" disclosure releases. Such documents have been used to justify almost any secondary use of medical data. These releases have permitted the disclosure of medical information to such bodies as pharmaceutical companies; employers, who seek health data concerning their firm's workers; the Medical Information Bureau, a nonprofit association that supplies insurance companies with medical information in order to prevent fraud; and direct market mailers.

¹¹ Alan F. Westin, Interpretive Essay, in Health Information Privacy Survey, supra note 1, at 7.

The protection for medical information is so weak in this country that marketing lists detailing the most sensitive information about citizens are for sale. Here is additional proof of the failure of current legal regulation. Johnson & Johnson has compiled a list for sale of five million elderly, incontinent American women.¹² Another company has advertised lists containing the names of six million allergy sufferers, 700,000 people with bleeding gums, and 67,000 people with epilepsy.¹³ Other citizens appear on a mailing list as suitable consumers of products intended for impotent middle-aged men.¹⁴

How did we get into the situation in which medical information is so poorly regulated that such lists are freely trafficked? Understanding the inadequacy of current regulation requires one to consider how the current patchwork of federal and state laws fail to control the application and use of medical data.

1. Federal Measures

On the federal level, data protection measures are found in constitutional law, the Privacy Act, and a few statutes that regulate narrow areas of data use. In any discussion of these measures, one must begin by noting that their coverage is

¹² See Larry Tye, List-makers draw a bead on many, Boston Globe, Sept. 6, 1993, at p. 12.

¹³ Id.

¹⁴ Just Lists Offers "Male Potency" File, DM News, April 19, 1993, at 37.

extremely limited. To begin with the United States Constitution, its protections apply only when there is action by the government. Yet, the overwhelming majority of most medical information in the United States is not in the hands of the government, but such entities as nongovernmental doctors and hospitals, insurance companies, and a variety of private sector computer networks. These private parties who control medical data are unlikely to meet the applicable tests for state action.

As for the Privacy Act, it protects only the data of federal agencies. In the 1980's, one expert estimated that this statute applies only to five percent of the medical data banks in the United States.¹⁵ Thus, federal measures leave most medical data entirely outside of their protections. In addition, there are notable weaknesses in each of these federal regulations. Let us begin with the applicable constitutional protections.

When the government does collect medical information, a constitutional right to informational privacy applies. Indeed, the constitutional right to informational privacy was first articulated in a case, Whalen v. Roe,¹⁶ that involved medical data. Whalen concerned New York State's plan to collect and store data relating to the prescription of certain drugs that had both legitimate and illegitimate applications. The Supreme Court found that the United States Constitution contained a right of

¹⁵ Terra Ziporyn, Hippocrates Meets the Data Banks, J. Amer. Med. Assn. 252 (20 July 1984) (quoting Professor Vincent M. Brannigan).

¹⁶ 429 U.S. 589 (1976).

informational privacy that prohibited "disclosure of personal matters" and protected "independence in decisionmaking."¹⁷ A number of important decisions of lower courts, such as United States v. Westinghouse,¹⁸ have applied this constitutional right to governmental attempts to obtain or examine medical information. The constitutional right of informational privacy has improved medical data protection in some instances. It has done so through application of its first branch, the nondisclosure interest.¹⁹ Yet, some lower courts have found that this element applies only to a narrow group of fundamental constitutional rights.²⁰ Indeed, some courts have viewed Whalen as a decision that sanctions all "legitimate" governmental requests for medical data.²¹ As to the second part of the right of informational privacy, the autonomy interest, it has been almost entirely absent from case law.²² There has not been a vigorous protection of medical privacy through application of it.

¹⁷ Id. at 598-600.

¹⁸ 638 F.2d 570 (3d Cir. 1980).

¹⁹ Mann v. University of Cincinnati, 824 F. Supp. 1190 (S.D. Ohio 1993); Doe v. Borough of Barrington 729 F. Supp. 376 (D.N.J. 1990).

²⁰ See, e.g., Walls v. City of Petersburg, 895 F.2d 188 (4th Cir. 1990).

²¹ See Gutierrez v. Lynch, 826 F.2d 1534, 1539 (6th Cir. 1987) ("legitimate requests for medical information do not constitute an invasion of the right to privacy").

²² Compare Plante v. Gonzales, 575 F.2d 1119 (1979) with Mann v. University of Cincinnati, 824 F.Supp. 1190 (S.D. Ohio 1993).

The limited constitutional protection to medical data has not been adequately supplemented by federal statutory measures. To begin with the Privacy Act, this law applies only to medical records in the control of federal agencies. This limited coverage is itself not without flaws. The most notable is found in the Privacy Act's limitations on secondary use. The Privacy Act prohibits the disclosure of records without the written request of "the individual to whom the record pertains."²³ There are, however, no fewer than twelve disclosure exemptions to this prohibition. Of these, the most problematic is the "routine use" exemption, which has been made into an enormous loophole.²⁴ Agencies have justified a wide variety of data disclosures as a "routine use" of personal information.

In addition to the Privacy Act, there are other provisions of federal law that provide some privacy protection for medical records. One such measure contains data protection measures for the social security records of the Department of Health and Human Services.²⁵ This statute does allow, however, for disclosures

²³ 5 U.S.C. § 552a(b).

²⁴ Id. at (b)(3).

²⁵ 42 U.S.C. § 1305. Social security records often contain a variety of medical information. This information is most typically collected in connection with claims for disability benefits. See generally Jerry L. Mashaw, *Bureaucratic Justice: Managing Social Security Disability Claims* (1983). A federal statute prevents "any officer or employee of the Department of Health and Human Services in the course of discharging" the social security program from disclosing any "file, record, report or any other paper, or information, obtained at any time by any person" from the Department. 42 U.S.C. § 1305.

"as otherwise provided by Federal law" and by regulations issued by the Secretary.

Federal law also protects the data of patients who are treated for alcohol or drug abuse in programs that receive federal funds or are subject to federal regulation.²⁶ These laws generally do a fine job of data protection.²⁷ Indeed, the best data protection for health information in the United States is provided for patients being treated for substance abuse in federally-funded clinics.

A good example of the success of these Federal statutes is

²⁶ 42 U.S.C. §§ 290dd-2, 290ee-3.

²⁷ For example, these laws permit disclosures of patient records only under certain specified conditions. There are four exemptions to the general standard of nondisclosure: (1) in accordance with the prior written consent of the patient; (2) to medical personnel to the extent necessary to meet a medical emergency; (3) to qualified personnel to conduct scientific research, audits or program evaluations; and (4) if authorized by court order.

This regulation guarantees confidentiality in order to encourage participation in alcohol and drug treatment programs.

Of the four circumstances in which information pertaining to alcoholism or drug abuse treatment may be released, 42 U.S.C. §§ 290dd-2, 290ee-3, the most important concern a court order and patient consent. As for disclosure pursuant to a court order, the judicial decision whether or not to release patient data is to be made pursuant to a balancing test. The statutory test requires judicial disclosure "after application showing good cause thereof," 42 U.S.C. § 290dd-2(b)(2)(C), and, more specifically, states, "In assessing good cause the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services." This balancing test is further developed by the applicable regulations. The statutory balancing test and the regulations have been carefully applied by a number of courts. These courts generally assess the seriousness of the alleged crime and check to see that redisclosure of the information will not occur beyond the immediate application necessary in the case at hand.

offered by the careful way they treat the issue of disclosure of patient information. Where broad releases signed by patients are used to justify third-party access to most medical data, these laws carefully define the conditions for the patient's "informed consent" to release of her data.²⁸ Written consent to a disclosure must include an explanation of such matters as: the purpose of disclosure; how much and what kind of information is to be disclosed; and a statement that the consent is subject to revocation at any time. Each disclosure must also be accompanied by a written statement that prohibits redisclosure. These statutes not only offer an excellent contrast to the kinds of "blanket" consent that generally takes place, but indicate the possibility for the success of additional federal data protection for medical information.

It must be emphasized again that these Federal protections generally apply only to the government. Only in strictly limited circumstances does federal law protect health care information in the private sector. Thus, private clinics for substance abuse that receive federal money are obliged to follow these federal rules for medical information, but privately funded clinics are not. For the most part, the treatment of health care information is the province of state law.

2. State Measures

The weaknesses in current federal data protection for

²⁸ 42 U.S.C. § 290dd-3.

medical information are not successfully overcome by existing state measures. To be sure, many different kinds of laws on the state level relate to medical information. Nevertheless, these measures do not create an effective system of data protection. To begin with constitutional law, some state constitutional provisions have been interpreted by courts, most notably in California, as setting limits on the application and dissemination of medical data.²⁹ The law of most states also recognizes a relationship between doctor and patient that gives rise to a general duty of confidentiality.³⁰ Some states have extended this duty of confidentiality to hospitals.

In addition, state statutes require certain reports concerning specific diseases or medical conditions to be filed with state health authorities by physicians, hospitals and laboratories. Such laws typically pertain to sexually transmitted diseases and other communicable diseases such as tuberculosis. State laws also require reports to be filed about knife and gunshot wounds and injuries to elderly individuals and children that might indicate elder or child abuse. Despite the highly sensitive nature of these data, these laws often do not contain specific limitations on the use that will be made of this information or put in place limitations on the time for which

²⁹ See, e.g., *Urbaniak v. Newtown*, 277 Cal. Rptr. 354 (1991); *Division of Medical Quality v. Gherardini*, 156 Cal. Rptr. 55 (1979).

³⁰ See, e.g., *Horne v. Patton*, 287 So. 2d 824 (Ala. 1974); *Hague v. Williams*, 181 A. 2d 345 (N.J. 1962).

these data will be stored.

Finally, a Uniform Health Care Information Practices Act has been drafted. This law has, however, been adopted in only a small number of states. Since the Uniform Act is subject to modification by state legislatures before passage, even widespread adoption of this law might not improve the nature of the protection for health care information.

Even within the same state, these many legal provisions have failed to impose a consistent framework on the application of medical information by primary care providers, supporting institutions, and secondary users. The lack of uniformity of regulation can also be found if one compares the legal systems of different states. Yet, flows of health care information take place on an interstate level. As one recent study of medical privacy has noted:

A state-by-state approach to regulation of medical information does not reflect the realities of modern health care finance and provision. The flow of medical information is rarely restricted to the state in which it is generated. Such information is routinely transmitted to other states, subject to differing legal requirements, for a wide variety of purposes ranging from medical consultation and research collaboration to governmental monitoring for quality.³¹

Whether as a result of regional health care alliances or an

³¹ Lawrence O. Gostin, Joan Turek-Brezina et. al, Privacy and Security of Personal Health Information in a New Health Care System, 270 JAMA 2487, 2489-90 (1993).

increased reliance on health data base organizations, national health care reform will cause even more transfers of medical information between different states.

The interstate flow of medical information calls for a federal response to these issues of data protection. This federal response must be embodied in a specific law that regulates the processing of health care data. In the 1985 Thomas Jefferson Lecture at the University of Pennsylvania Law School, Professor Spiros Simitis, an international data protection expert, urged an abandonment of any search for "abstract, generally applicable provisions" in favor of "a context-bound allocation of information embodied in a complex system of both specific and substantive regulations."³² Such a system of regulations is offered by Representative Condit's fair information practices bill for health information.

Moreover, these fair information practices must be put in place now as part of national health care reform-- not at some date in the future. Yet, the Clinton Administration's Health Security Act (H.R. 3600, S. 1757) foresees first the establishment of an electronic data network of health care information (Sec. 5103) and then, some years later, the creation of "a comprehensive scheme of Federal privacy protection" (Sec. 5122). This scheme, which is to include fair information practices, is to be submitted to the President and Congress

³² Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. Penn. L. Rev. 707, 742 (1987).

within three years of the enactment of the Health Security Act.
(Id.)

We cannot wait for data protection in this fashion. In an age of rapid technological change, privacy lost is not frequently regained. The law must structure fair information practices at the same time as it authorizes the collection and retrieval of personal information. In the case of health care information, this conclusion has also been reached by the Committee on Regional Health Care Services of the Institute of Medicine. The Committee not only advocates the enactment of a federal fair information practices law, but has urged Congress to act "as soon as possible."³³

II

International Developments

There is a great need for improvement of the regulation of medical privacy in the United States. Developments in Europe provide an important example in this area as well as an independent, additional ground for passage of a fair information practices act for medical information in the United States. I wish now to discuss how national and European-wide laws regulate the processing of medical data, and then analyze how the inadequate protection of medical data in the United States can lead to the blocking of the transfers of personal information to our country and limit the ability of American companies to

³³ Institute of Medicine Study, supra note 9, at 191.

process European records.

Within European nations, medical data are generally subject to a variety of legal measures. In most European nations, in contrast to the United States, data protection proceeds at an initial level through an omnibus law that regulates the public and private sectors alike.³⁴ These laws are then supplemented and strengthened by other general laws and sectoral measures that contain more precise regulations for individual areas of processing activities. Thus, in the Federal Republic of Germany, medical data are subject to the Federal Data Protection Law,³⁵ the Code of Social Law (Sozialgesetzbuch),³⁶ the Criminal Code,³⁷ and state data protection laws.³⁸ In the medical sector, the resulting level of data protection in Europe, although not without flaws, is generally at a higher level than in the United States.

The level of protection for medical information within any

³⁴ David H. Flaherty, *supra* note 3, at 21-39; 93-103; 165-174.

³⁵ Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990, BGBl. I, 2954 [hereinafter cited as BDSG].

³⁶ Sozialgesetzbuch vom 11. Dezember 1975, BGBl. I, 3015.

³⁷ See Strafgesetzbuch (Criminal Code), § 203(1) (forbidding doctors from violating the "private secrets" of others).

³⁸ Some state data protection laws contain specific provisions concerning health care information, see, e.g. Hessisches Datenschutzgesetz (Hessen Data Protection Law), vom 11. November 1986, § 34(6). German states are also in the process of promulgation of sectoral laws for health care information.

European nation is also affected by a European-wide treaty. The Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Data, which currently is the most important European agreement for data protection, requires that signatory nations only permit the processing of sensitive data, including "personal data concerning health," when "domestic law provides appropriate safeguards."³⁹ These safeguards include: rights of access and correction; a specification of collection purpose; data security measures; and limitations on unnecessary data collection and data applications that are incompatible with the original collection purpose.⁴⁰ In addition, remedies are to be provided in cases of lack of compliance with requests for: information about collections of personal data; access to personal data; or correction of personal data.⁴¹

This general provision of the Convention has been expanded upon by the Council of Europe's Recommendation No. R(81)1, which provides sectoral regulations for automated medical data banks.⁴² These regulations provide additional specifications of

³⁹ Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, no. 108 (January 28, 1981), Article 6.

⁴⁰ Id. at Articles 5, 7, 8.

⁴¹ Id. at Article 8(d).

⁴² Council of Europe, Regulations for automated medical data banks, Recommendation No. R(81)1 (January 23, 1981). The Explanatory Memorandum to the Recommendation states, "the operation of every automated medical data bank [should be] subject to a specific set of regulations. The general purpose of

the necessary data protection principles to be applied to medical data banks. The Recommendation states that its requirements "are to be taken duly into account not only with regard to medical data banks which are operational, but also those which are in the development phase."⁴³ Taken together, the Convention and the Recommendation reflect a serious European-wide commitment to data protection in the medical domain.

In addition to the Council of Europe's Convention and Recommendation, the treatment of medical data within Europe will soon be affected by the Commission of the European Community's Directive on Data Protection. An amended draft of this document provides insights into Europe's likely final approach to medical data protection.⁴⁴

Like the Convention, the Draft Directive requires member countries to establish legislation that conforms with its standards. Its goal is to ensure a "high level of protection" within the Union for "fundamental rights and freedoms, notably the right to privacy."⁴⁵ The Directive stresses that fair information practices must be in place before member states

these regulations should be to guarantee that medical data are used not only so as to ensure optimal medical care and services but also in such a way that the data subject's dignity and physical and mental integrity are fully respected." *Id.* at 13.

⁴³ *Id.* at 1.5.

⁴⁴ Commission of the European Communities, Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM(92)-- SYN 287.

⁴⁵ Preamble at (1).

permit the processing of personal information, including the processing of "data concerning health."⁴⁶ To put it another way, without sufficient data protection laws, medical information may not be processed.

The proposed Directive and the Council of Europe's Convention are of great significance. The importance of these two documents is, in the first instance, as a positive example of data protection measures for medical data. They are also important because of their setting of rules not only for the processing of personal data within the European Union, but also for the transfer to these data to any "third country," such as the United States.

The Council's Convention and the Union's Directive permit the prohibition of data transfers, including medical information, to countries with poor data protection. According to the Council of Europe's Convention, data exports may be prohibited to nations that do not offer "equivalent protections" for personal information.⁴⁷ As to the Draft Directive, it gives responsibility to each national government within the Community to oversee the conditions of transfers to non-Community nations. The Directive's critical requirement is that data transfers be permitted "only if the third country in question ensures an

⁴⁶ Id. at Article 8.

⁴⁷ For analysis of this provision of the Convention, see Joel R. Reidenberg, The Privacy Obstacle Course, 60 Fordham L. Rev. 161-62 (1992).

adequate level of protection."⁴⁸ The adequacy of protection is to be "assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations."⁴⁹ Among the circumstances to be assessed are "the legislative provisions . . . in force in the third country in question."⁵⁰ The adequacy of protection can also depend on "professional rules," which can include a given company's business practices or code of conduct.⁵¹

Data exports can also be blocked under the national law of various European nations. In Germany, for example, the Federal Data Protection Law requires consideration of the level of data protection in a third country before any international transmission of personal information.⁵² Such analysis must be carried out in cases of transfer by the government and private companies alike. In cases of non-governmental transmissions, a private company can make itself liable for fines and even criminal penalties for transmissions to countries with

⁴⁸ Draft Directive, at Article 26(1).

⁴⁹ Id. at Article 26(2).

⁵⁰ Id.

⁵¹ Id.

⁵² BDSG, §§ 17, 28. For a discussion of the need for equivalent protection before the transfer of personal data from Germany to a foreign country, see Spiros Simitis, §1 (Räumlicher Geltungsbereich), in *Kommentar zum Bundesdatenschutzgesetz*, § 1, Rdnr. 74-107 (Spiros Simitis, Ulrich Dammann et. al. eds., 4th ed. 1992).

insufficient protections.⁵³

What do these provisions for blocking data exports under the Council of Europe's Convention, the Union's Directive, and national laws mean for the United States? They indicate that transfers of personal data from Europe to this nation will depend on the adequacy of protection that these data receive once they are here. This decision is likely to be made by looking at the kind of transfer and the nature of the protection that is offered by the legal order as well as the business practices in the state to which the data is sent.

Medical data likely to be affected by these measures are found in employee information in the control of international corporations and drug research studies, which pharmaceutical companies now carry out in many countries as they seek world-wide approval of their products. Moreover, there is now an international industry in information processing. As a result, American companies compete globally for contracts that will involve the processing of health information. It makes good business sense for the United States to institute federal measures of data protection for medical data.

III

Data Protection Oversight

Passage of a fair information practices bill would greatly improve the level of data protection for medical information in

⁵³ BDSG, §§ 43, 44.

this country. This legislative activity should also be accompanied by passage of a bill creating a federal data protection board. The idea of creating such an institution has been around since the debate preceding the creation of the Privacy Act in 1974, but it is likely today to receive particularly strong support from the American people. Concern about privacy is high in the United States. In fact, according to a 1993 poll conducted by Louis Harris and Associates, eighty-six percent of the public favors the creation of an "independent National Medical Privacy Board to hold hearings, issue regulations, and enforce standards."⁵⁴

Even more useful than a board devoted solely to data protection in the medical sector would be an institution that was empowered to consider the effects and implications of data processing practices in other contexts. Bills to create such a general data protection board are currently before the House and the Senate of the United States Congress, and I urge passage of such a measure. In its attempt to protect individual self-determination, data protection law can remain effective and current only if such an institution exists to assist government bureaucracy, the legislature, the business community, and the data subject.

The creation of the United States Data Protection Board is of particular importance for the protection of informational self-determination in an era of rapid technological change.

⁵⁴ Health Information Privacy Study, *supra* note 1, at 101.

Indeed, the greatest changes in personal data use anywhere in the United States are likely to take place in the medical sector. There is an acute need for a governmental body with the institutional expertise and continuity of interest to monitor the impact of changes in this area on individual privacy.

A Data Protection Board would monitor data processing practices and compliance with laws, draw the attention of the legislature and the public to the problems of existing laws and the need for further regulation, assist citizens seeking to protect their interests and exercise their rights, and help business in understanding national and international legal developments. By fulfilling these tasks, the data protection commission would help to ensure that public administrative bodies, the legislature, citizens and the business community remain aware and active as the conflicts generated by information technology change.

A further role of a Data Protection Board would be to represent American interests and assist American companies facing scrutiny by foreign data privacy authorities. Almost all other Western nations have created such data protection boards. Indeed, the European Union's Draft Directive requires each member state to "designate an independent public authority to supervise the protection of personal data."⁵⁵ Significant formal and informal contacts now regularly occur between the world's data protection commissions.

⁵⁵ Draft Directive, Article 30.

The United States must do more than fight for a principle of free international data flows; it must develop the institutional expertise that will allow involvement in the worldwide debate over data protection concerns. One reason for the United States' current, minimal role in this international discussion has been its lack of any Data Protection Board. Creation of such an institution would dramatically improve the representation of our nation's interests abroad. Independent monitoring of the effects and implications of information technology and data processing practices is necessary both to protect citizens' informational self-determination and to maintain the flow of data exports to the United States.

Mr. CONDIT. Thank you, professor, for that excellent testimony. We appreciate your input. I have a few questions and then we will try to get you out as quick as we can.

The Clinton health bill includes a one line provision prohibiting any use of health data in making employment decisions. H.R. 4077 does not touch that issue. Could you discuss some of the complexities of regulating employer use of health data?

Dr. Barker.

Dr. SEPULVEDA. Mr. Chairman, let me make a comment on that.

In employer-provided occupational health services, there are a broad range of encounters with employees that involve the collection of personal health information that are unrelated either to the provision of health care, to treatment, to billing or payment.

A previous member of the first panel commented on the importance of broadening the definition of protected health information. Let me give you some insight into the extent of these nontreatment, payment-related encounters, and they are largely prevention oriented.

These are prevention-oriented activities that relate to health promotion and wellness programs that might include health counseling, the administration of health-risk appraisals, health education, consultation and referral; injury and illness prevention programs that can involve physical assessments, they can involve the personal evaluation of the health of a work environment, too, or actual physical performance of work of an individual, discussions pertaining to individual health concerns, about physical, chemical or biological aspects of their work environment.

It includes periodic examinations, counseling pertaining to international assignments and health issues that are raised in that context regarding the availability of health care for specific medical conditions for themselves or their dependents in other countries, which can pose enormous problems for individuals going overseas, and also the provision of guidance to managers who are responsible for implementing accommodations or modifications of a work environment to permit an individual with a given medical condition to safely and productively perform work.

It is my personal view that some statement to the effect that it isn't just a provision of and payment that defines protected health information, but activities related to the evaluation of health status would provide language to cover these kinds of activities. These are some of the areas that are impacted in the workplace as they pertain to the interaction between employers and employees and health and health information.

Mr. CONDIT. Would you want to see H.R. 4077 extended to the workplace records that you have just discussed?

Dr. SEPULVEDA. From the perspective of a multistate employer and given the uniform nature of Federal law, yes, Mr. Chairman, it may be helpful.

Mr. CONDIT. Any other comment to that?

Mr. SCHWARTZ. There is an absolute need to protect employee data. The problem with the current system is that since, in many cases, the employer is paying for the health care, the insurer will on a routine basis turn information over to the employer. But that will also differ from State to State.

In California where there is a constitutional right to information privacy, in article 1 of the California Constitution, courts have interpreted that as providing protection for employee health care data. But normally under the current system that information is not protected.

Mr. CONDIT. As far as we can tell right now, H.R. 4077 does not appear to affect the Americans with Disabilities Act. Do you agree with this analysis and that this is the correct policy?

Mr. BOLAN. I will just say that Medic Alert itself has not looked at this, but I am generally familiar with the ADA and did review the bill with that in mind, and concur with your point of view that it isn't impacted and we wouldn't have any recommendation that it should change.

Dr. SEPULVEDA. Mr. Chairman, there is language in one of the questions in your executive summary, and the answer that ought, also, I believe, to address other Federal legislation that has similar implications, specifically the Occupational Safety and Health Act, and the Mine Safety and Health Administration responsibility—that is that there are requirements in some standards, particularly for recordkeeping, that require the provision of personally identifiable health information. And so there is a gap in the obligations for trusteeship in the language of your current legislation. And the requirements for compliance under those standards that can be remedied by perhaps adding these to the language of your answer to question 13, that says something to the effect: That there is nothing in the bill that is inconsistent or will disturb the rules set forth in the Americans with Disabilities Act, and perhaps also in the OSHA Act.

Mr. CONDIT. Thank you.

Mr. Bolan, there has been much discussion about the use of the "smart card" and their value in emergency situations. What does Medic Alert experience tell us about the value of wallet cards?

Mr. BOLAN. Thank you.

Medic Alert has quite a bit of experience with wallet cards and has had quite a lively discussion at board meetings recently about the potential of "smart cards." We translate "smart cards" into "smart bracelets." Our experience is that wallet cards are generally not found. There could be many awkward situations involving the person who first arrives on the scene. There could be some questions about why this person might be looking in a wallet, and so forth. Emergency rooms see the bracelet as the identifier. They do not typically find or use wallet cards.

But with regard to the smart technology. Unfortunately if it were in the bracelet, it is perishable technology, it might be more relied on than a phone call to the central data bank. So our board has had quite lively discussions on the potential of a "smart chip" in a bracelet, and thus far has decided against moving in that direction.

Mr. CONDIT. Is it because of the cost?

Mr. BOLAN. No, it is because of the potential to rely on information that is then out of date.

Mr. CONDIT. Does anyone else have comments to that?

Dr. BARKER. As I made reference, Mr. Chairman, we are obviously working on "smart cards" very actively. The technological dif-

ferences of what we can do on bracelets versus what we can do on cards is something that will evolve. But clearly, miniaturization means we can put considerable health care data on either or both.

We believe that data encoded in "smart cards" can be of great value not just in an emergency situation but in a routine situation. And the encryption techniques that are available now mean that we can be assured of the security of the data, which are more secure on a card than they would be on a piece of paper.

Mr. CONDIT. Mr. Bolan, disclosure for emergencies are a troublesome issue. These disclosures happen under circumstances that necessarily make it difficult to be certain. There is evidence from Canada that there have been abuses. How do we build in enough flexibility so that recordkeepers can do the right thing?

Mr. BOLAN. That is from a Medic Alert standpoint undoubtedly the most difficult issue. Medic Alert recommends and looked carefully at section 126 to see whether there would be proper protection in the instance that a rapid response to a request for emergency information was provided and it turned out the person making the request misrepresented himself.

What Medic Alert would recommend is that there be a clear protocol, as we have, to identify and verify the person making the request and that if that verification is made and the information is provided in good faith, then the information should be able to be provided in that manner, in good faith. If the person making the request for the emergency medical information made a fraudulent request for that information and misrepresented him or herself, then the onus should be on that individual rather than on Medic Alert or any other organization having supplied the information, for any penalties.

Mr. CONDIT. Mr. Horn.

Mr. HORN. Thank you, Mr. Chairman.

We have got several of you here that are real experts on modern technology data bases, interactions between them and interactions with competing systems. I am curious if a public-run data base is established for one health plan or another, or even for medicare, as we have now, to any degree, would every medical facility be required to operate from the same technology, either hardware or software?

Where are we in assuring compatibility of different systems now and how much of a problem is that?

Dr. BARKER. The problem lies not so much in the hardware technology but in the standards and the formats in which the data is kept. Currently, even within a single hospital institution, data are stored in many different formats, for many different purposes.

As we build toward integrated systems of care and then beyond to State and national levels, we desperately need to converge on standards for the way the information is held, formats for clinical data and administrative and financial data, if these large systems of care are really to operate efficiently.

Mr. HORN. On the software of medical records, for some reason, which I have never thought had that much merit—if I were Secretary of HHS, I would have let them sue me. Secretary Sullivan, as you recall, tried to get all competing providers of the insurance

industry into the same room to get some agreement on coding and this kind of thing. I have lost track of how that is going.

It makes great sense. People feared the antitrust laws in this area. To me as a former administrator, you get them in the room and say, does last name go first or last and you go right down, how many types of cancer, how many code numbers can we agree on, et cetera. Because there is no question in the medical profession nationwide each doctor now runs a small business of which he has several clerks, if you will, simply to copy with the unbelievable number of different types of forms coming at them.

Obviously, in an electronic age, everybody is going to be looking for some simple way we can get compatibility of agreement on what are we putting in the data.

Any advice on that?

Do you see the groups getting together?

Are there any problems with existing laws?

Dr. BARKER. My only comment is I think we will not get there in one leap. We see a range of discussions both in the payor community and the provider community, which I think will get us painfully toward the kind of uniformity you talk about, absent a single-payment system, for example.

But that is only part of the problem. We are obviously working actively with our customers and with all of the groups that are involved in this to seek to develop that kind of standard.

The WEDI report identified something between \$25 and \$30 billion of administrative waste you can eliminate from the health care system if you can automate the key transactions. But we don't see this coming to pass in a single leap in the next couple of years I am afraid.

Mr. HORN. Anybody else?

Mr. BOLAN. Mr. Horn, I wonder if I could concur with the point of view that it is a two- or three-step process. Rapid passage of H.R. 4077 with an early implementation date would certainly create incentives for the managers of information systems to come to whatever voluntary system best served their various needs. And so passage of this bill would be a good first step.

Mr. SCHWARTZ. I think another reason for passage of the bill, if we have a situation where different technologies are being developed and discussed, I think it's important to get the rules of the road as far as fair information practices are in place as the systems are developed, so that they will all be compatible with your bill.

Mr. HORN. That's a good suggestion.

Now, one of the things we talk about in all sorts of health care legislation, is using the information developed in the course of medical examinations, medical procedures and processes, to run output analysis. I'm curious, in terms of data bases performing the analytical as well as the operational functions, and with particularly the role of research by outside researchers on medical records, and the degree to which you've looked at this in your own situations in terms of either the IBM employee data base, to what degree do you feel you have problems making data available for scholars, and people interested in everything from administrative efficiency to actual outcomes of particular types of treatment over a longitudinal time period?

What are the problems there, and have we covered some of those?

Is there something else to be done?

Mr. BARKER. I leave that for Dr. Sepulveda to talk about our policy in terms of release of such information. I can only reiterate the value of it.

Medical practice should be a continuous process of learning, but currently in practice, we don't learn from this experience. Outcomes analysis is going to be an enormously important part of the benefit that will come from the electronic keeping of medical records and analysis of these medical records. This bill will facilitate that.

It has to be said on the subject of outcomes that there's a great deal of talk about "outcomes." While most people mainly collect information on inputs. There's a great deal of very basic work to be done on defining the parameters of productivity in health care so that both a realistic assessment of health status and of customer service can be collected in a way that all institutions would recognize as valid.

But perhaps I could refer to Dr. Sepulveda on our own medical records.

Mr. HORN. Please, Dr. Sepulveda.

Dr. SEPULVEDA. Yes, Mr. Horn.

IBM does not routinely engage in health research involving either the benefits claims sphere of health information, or its employee medical records sphere of information. Having said that, we do provide as part of our preventive orientation in IBM, some periodic examinations for subgroups of employees who are engaged in activities for which we think it is prudent to provide ongoing evaluation of potential health effects.

Those periodic examination programs are largely voluntary. Some are required by law in some OSHA standards.

We review that information individually with employees as the information is collected and as results are acquired. We also try and understand that information from an aggregate perspective.

On rare occasions, there is medical research conducted involving the IBM work force. It comes in two flavors. We recently announced in 1993 the result after nearly a 5-year study by the Johns Hopkins University School of Hygiene and Public Health on the reproductive health of men and women in our semiconductor fabrication facilities.

The desire to have that work done was a consequence of questions that were raised about safety in those environments, and a cluster of miscarriages at another computer manufacturing company nearly 6 or 7 years ago. We independently invited universities to come forward and propose ways in which those questions could be answered.

The Johns Hopkins University was selected and the process for undertaking that research was a process that was largely dictated by the rules overseeing the conduct of research at the Johns Hopkins University. And so the interface, the data collection, the analysis, and so forth, are all circumscribed by the rules governing research at Johns Hopkins University.

Mr. HORN. Yes, Mr. Bolan.

Mr. BOLAN. Mr. Horn, I appreciate the question, and I'd like to respond, if it's acceptable to you, from the standpoint first off of my employment organization, and then back to Medic Alert's point of view of this.

The medical societies and many other organizations will have many, many instances in which medical information is collected at a variety of places, is then accumulated into a central health outcomes data bank of one type or another. We do that right now.

And the question arises, let's say, a hacker gets into the system somehow and extracts information for an inappropriate use. Should the information have been masked from the standpoint of every single individual site where the information was going in so that its name and address information was removed from the record before it went into the system? Or should it be the responsibility of the receiving agency? A public health trustee is defined as one who either receives or transmits, among others.

Medic Alert's recommendation to the subcommittee is to proceed with enactment of this legislation. My personal view is that if the subcommittee tries to define all of these various circumstances, it will cause years of delay before the bill is "perfect."

On the other hand, if H.R. 4077 is enacted and the rulemaking process tries to define every one of these circumstances, that also will cause years of delay. On the other hand, if the rulemaking process moves forward reasonably rapidly and we have certain situations that require testing through the courts, that also will be years. But that's the best choice, because in the meanwhile, most all medical records will have been protected.

Mr. HORN. Very good.

Professor Schwartz.

Mr. SCHWARTZ. Yes, I think if we back up and we think about the technological change that's occurring, it's clear that because we're reducing information that was once in files and in paper format to a digital format, it's going to have the same effect that we saw at the turn the century when they decided to put automobiles on an assembly line and move them around.

We now have information that can be reduced to a flow. And that means it can be used for many, many purposes and there's going to be a great desire to apply this information for health research. And as a matter of fact, I think the traditional distinction between using the information for treatment and research is breaking down, because it is in this digital form where it can flow from source to source.

What is necessary, then, is to have some kind of fair information practices that are in place, and I think section 128 of the bill does a pretty good job of doing that, and then regulations can certainly tighten it up and add additional specifications.

Mr. HORN. Well, thank you. I have appreciated all of your testimony.

And, Professor Schwartz, since I am a former university professor and president, I thought your paper with simple declarative sentences leading each paragraph was extremely well done and you ought to be a professor, not Associate Professor Schwartz.

Mr. SCHWARTZ. I'll pass that on to my dean.

Mr. CONDIT. Mrs. Thurman.

Mrs. THURMAN. Professor Schwartz, since you started this up on the basketball team, I just have to carry that, because this may not be about your basketball team, but maybe about your fans, since I represent the University of Florida. One of the things that we found at the actual final four was that we were all rooting for Arkansas because they were an SEC team, but you all were rooting for Duke, which was an ACC team.

So could you explain why that happened?

Mr. SCHWARTZ. I'm in trouble now.

Mrs. THURMAN. We'll remember it next year.

Mr. SCHWARTZ. OK. And I think I'm allowed to say that I'll seek further—

Mr. HORN. You are under oath.

Mr. SCHWARTZ. I think I can seek further counsel and respond to that at a later date.

Mrs. THURMAN. Just remind those folks at Arkansas that we were really with them, so we would appreciate their support next time.

Mr. SCHWARTZ. Absolutely.

Mrs. THURMAN. Professor Schwartz, in your testimony you talked about European countries having more comprehensive privacy laws than we have here in the United States. Are these privacy codes accomplishing their goals without creating a lot of confusion and interference with routine activities?

Mr. SCHWARTZ. Yes, I think that's fair to say. Now that doesn't mean that there's not complaints and that it's not a process of compromise and accommodation. But I don't really see either economies collapsing because of that or research grinding to a halt. And as a matter of fact, there are instances in which, because of a rationalization of data processing practices, money has actually been saved.

Mrs. THURMAN. OK.

Would a data protection board take the responsibility just for the health bill or would it have other functions?

Mr. SCHWARTZ. I think that the best approach is to take the approach that Senator Simon does in his bill, and rather than have a very narrow sectorial board, to have a general board in place that can look at these issues and other issues. Because I think one thing that happens is there is such overlap between different kinds of applications of medical data. If we only have a very specifically focused board, there may be things that fall through the gaps.

Mrs. THURMAN. OK.

Are the protection boards in other countries, are they large and expensive regulatory—because we always hear from our constituents about more regulation and more this and more that. I mean, do you see these as being expensive and kind of far reaching or—

Mr. SCHWARTZ. No, they have been able to be kept relatively small in European countries. In the countries where there is more of a registration function of these boards, they tend to have been caught up in more sort of bureaucratic things and bogged down in that.

In countries, such as Germany, where there are no registration functions of the boards, they are allowed to be more of an oversight

agency. They have been kept relatively small and relatively inexpensive.

Mrs. THURMAN. In your testimony, you talk about Whalen versus Roe. Do you believe that there's any hope in this after, or because of this decision, that we might someday obtain better protection for health records in the courts?

Mr. SCHWARTZ. Well, the first thing to say about Whalen versus Roe, it is, of course, a Federal Constitution decision. And it will only apply where there is State action. Because our constitutional rights in this country only apply where there is State action, because that's the kind of Constitution we have. Therefore, it's never going to apply to private actors. And so even if we get better application of the constitutional right to informational privacy in this country, it's not going to apply to the private sector. And that means we need a Federal statute, such as the one that is before this committee.

Mrs. THURMAN. OK. Thank you.

Appreciate you all being here.

Mr. CONDIT. Ms. Ros-Lehtinen, do you have any questions?

Ms. ROS-LEHTINEN. I am sorry, Mr. Chairman, I do not.

Mr. CONDIT. Very good.

We appreciate you gentlemen being here today. You've been most helpful to the subcommittee and we will be in contact with you if we have additional questions.

Maybe you can respond to those in writing.

Thank you for your input.

This meeting is adjourned.

[Whereupon, at 11:58 a.m., the subcommittee adjourned, to reconvene Thursday, May 5, 1994.]

THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1994

THURSDAY, MAY 5, 1994

HOUSE OF REPRESENTATIVES,
INFORMATION, JUSTICE, TRANSPORTATION,
AND AGRICULTURE SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:35 a.m., in room 2247, Rayburn House Office Building, Hon. Gary A. Condit (chairman of the subcommittee) presiding.

Present: Representatives Gary A. Condit, Karen L. Thurman, Lynn C. Woolsey, Craig Thomas, Ileana Ros-Lehtinen, and Stephen Horn.

Also present: Robert Gellman, chief counsel; Aurora Ogg, clerk; and Diane Major, minority professional staff, Committee on Government Operations.

Mr. CONDIT. Good morning. This is the third and last series of hearings on the Fair Health Information Practices Act. We have generally had positive testimony about the bill from the administration, the medical establishment, and others. While I know there is still a lot of work to be done on the bill, the reviews are encouraging.

Today's witnesses are from the health advocate and public interest groups. We are likely to focus attention on some of the more difficult aspects of the legislation and I look forward to their testimony this morning.

We are delighted this morning to have our colleague with us, Representative Tom Sawyer, chairman of the Census Subcommittee of the Post Office and Civil Service Committee. Mr. Sawyer is leading a group of members who are working on health information systems legislation. This involves a set of issues that overlap, in part, with the privacy issue.

We have been working very closely together to coordinate our efforts and we are delighted to have him here and we are delighted to have his participation in this issue and his leadership.

Representative Sawyer.

STATEMENT OF HON. THOMAS C. SAWYER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. SAWYER. Thank you, Mr. Chairman. I am grateful for the opportunity to be here with the subcommittee. The work that you have done has been noted for its diligence and quality in an attempt to write legislation in a difficult and complex arena.

The bill that you are working on goes a long way toward giving Americans the kind of protections that they frankly have not had before. Although many believe that their health care histories are private, confidential, and secure, in large measure they are not, today.

Last fall, our colleague, Dave Hobson, and I introduced H.R. 3137 to set out a process for building a national health information infrastructure. We are working to strengthen many provisions, as you are in your bill, based on testimony and other expert advice.

We believe that with an electronic network, we can look forward to less paperwork, the capacity to detect fraud, the development of a wealth of useful data to support policy analysis, planning, and general research and other statistical applications.

We cannot build that kind of system without privacy safeguards and that is where I hope we can create a constructive partnership. We want the structures and functions envisioned in our bill to be governed by the requirements in your bill and, in that way, to make them work together.

I am grateful for your support and encouragement and that of your staff. I think we have come a long way.

I would like to focus my discussion today on a particular area—the role that research and statistical applications of data can play in a well-run health system and how we should allow access to information for such appropriate and well-controlled research activities. That access is going to help us plan for the consequences of the enormously rapid changing demographics of this nation, a kind of change that is going to affect everything that we might do, no matter what kind of health care reform we choose to enact.

There is an urgent need to standardize data and to provide more efficient and cost-effective business practices. You cannot do one without the other. The new technologies allow information to flow more economically than before, perhaps more easily than before, and so we must make sure that it flows with greater care than before.

The changes will give us, for the first time, the chance to use the resulting data for research in an affordable and practical manner. As a result of this, we will probably understand better barriers to care, cost, and financing issues, discrimination in kinds of care, and their implications on specific segments of our population.

I would like to offer, for your consideration, language that your staff has reviewed, to ensure that the definition of “allowable health research” allows for the full range of that kind of important, policy related research undertaking.

With this kind of opportunity, however, comes substantial risk. There have to be clear and enforceable limits on who has access to data, what kind of data they have access to, and for what purposes. The public has to have confidence that we are serious about the business of protecting its privacy.

I believe that implementing the principle of functional separation, as articulated by the Privacy Protection Study Commission of 1977, is one important way to ensure that we set reasonable limits. Functional separation is the principle that data used for research or statistical purposes should not be used to effect any individual directly, either positively or negatively. It is just simply inviolate.

In other words, data about a person aggregated with information about others could tell us something important about our society but not about that individual or his or her eligibility for benefits or compliance with the law or any purpose.

Individually identifiable data are sometimes needed to conduct research, but the research results should never include data in individually identifiable form. That protection is especially needed when data are linked together to create new sets of information which, in the end, could well be more sensitive than the individual data were, separately.

One practical way to implement this principle is to require that data given to a research or a statistical agency cannot be disclosed for any nonresearch or nonstatistical purpose. The model that we have been thinking of in trying to craft this legislation is the Census Bureau's handling of data from its censuses and surveys.

Title 13, United States Code, prohibits that data from being disclosed for any purpose whatsoever, even to another government agency. There have been a number of attempts over the years to penetrate that prohibition for what might seem, on first glance, to be worthwhile purposes, like law enforcement, but that inviolate standard of protection has never been breached. I think that same kind of standard ought to apply here.

I believe that your bill does a good job of implementing functional separation and it might be useful to have an even more explicit expression of what that principle means. I would argue for the most stringent protection and the most stringent penalties for those who would try to break down that wall.

In an electronic environment, that wall may not exist in a purely physical sense, at least not the way it did when we enacted the laws years ago that governed the Census Bureau. But a physical wall alone would not be adequate in the modern environment. We have to make sure that a wall exists in a computerized environment in which our personal data will increasingly reside.

Technology can help us strengthen, rather than weaken, that ability to protect confidentiality. We can make sure that it is accessible only to those who are authorized. We can keep track of who is seeking information and who gets it. In that way, we can assure, even better than we do today, that we have the capacity to enforce suitable legal protections.

I think that, working together, we can achieve that kind of strong privacy protection for personal health information. I look forward to continuing to work with you toward that end.

[The prepared statement of Mr. Sawyer follows:]

Statement
of Congressman Tom Sawyer

before the Subcommittee on Information, Justice,
Transportation and Agriculture
Congressman Gary Condit, Chair

May 5, 1994

Mr. Chairman, thank you for the opportunity to offer my thoughts on the critical role privacy legislation will play in health care reform.

I want to join other witnesses in applauding your diligence in writing legislation to address a difficult and complex issue. Your bill goes a long way toward providing Americans with protections they have not had before. Although many believe that their personal health histories are private, confidential, and secure, they are not.

Last fall, Congressman Dave Hobson and I introduced H.R. 3137, the Health Care Information Modernization and Security Act. That legislation sets out a process for building a national health information infrastructure. We are working to strengthen many provisions, based on testimony and other expert advice.

With an electronic network, we can anticipate less paperwork, an enhanced ability to detect fraud, and a wealth of useful data to support policy analysis, program planning, and general research and statistical uses.

However, we can't build such a system without sound privacy safeguards. That's where I hope we can create a constructive partnership. We want the structures and functions envisioned in our bill to be governed by the requirements in your bill. We are grateful for the support and encouragement of you and your staff during this process.

Today I want to focus my comments on one specific area of your legislation: the role that research and statistics should play in a well run health care system. We must allow access to information for appropriate research and statistical activities. That access will help us to plan effectively for the consequences of a rapidly changing demographic landscape that clearly will affect the implementation of a new health care delivery system.

Health care providers are recognizing the urgent need to standardize data to create more efficient and cost effective business practices. New technologies allow information to flow more economically than ever before. Those changes will give us the ability, for the first time, to use the resulting data for research and statistics in an affordable and practical manner.

As a result of this new availability, we will better understand barriers to care, cost and financing of care, discrimination in types of care, and their implications on the elderly, disabled, children, minorities, and other segments of the population. I want to offer, for your consideration, language that your staff has reviewed to ensure that the definition of allowable health research permits for the full range of important policy-related research projects.

With this bounty of opportunity comes some risks. There must be clear and enforceable limits on who has access to data, which types of data, and for what purposes. The public must have confidence that we are about the business of protecting their privacy.

I believe that implementing the principle of functional separation, articulated by the Privacy Protection Study Commission of 1977, is one important way to ensure that we set reasonable limits. Functional separation is the principle that data used for research or statistical purposes should not be used to affect any individual directly, either positively or negatively. In other words, data about a person are aggregated with information about others to tell us something important about our society, not about that individual's eligibility for benefits or compliance with the law. Individually identifiable data are sometimes needed to conduct research, but the research results should never include data in individually identifiable form.

That protection is especially needed when data about a person are linked together to create a new set of information, which may be more sensitive than the original pieces. For example, to determine if we can afford to alter the entitlement age for both Medicare and Social Security, one must link information about the affected population and health insurance costs. This type of analysis is currently conducted using Medicare records and survey data linked together.

The practical way to implement this principle is to say that data given to a researcher or a statistical agency cannot be disclosed for any non-research or non-statistical purpose. The model I find most suitable is the Census Bureau's handling of data from its censuses and surveys. Title 13, United States Code, prohibits that data from being disclosed for any purpose, even to another government agency.

Although there have been many attempts to penetrate these files for what might seem on first consideration to be worthwhile purposes (such as law enforcement), that inviolate standard of protection has never been breached.

Once again, I believe your bill does an reasonable job of implementing functional separation. If I were to recommend any change, it might be an even more explicit expression of that principle. I would argue for the most stringent protection of those data and the most stringent penalties for those who would try to break down the wall we erect between data for research and data for other purposes.

In an electronic environment, that wall may not exist in a purely physical sense, like it did when we enacted the laws governing the Census Bureau. In fact, a physical wall alone would be inadequate. However, we must make sure a wall exists in the computerized environment in which our health data will increasingly reside.

While technology compels us to reconsider how we collect and store information, it actually can strengthen, rather than weaken, our ability to protect the confidentiality of data. We can ensure that information is accessible only to those who are authorized to use it for a given purpose. We can keep track of who's seeking access and who gets it. To complement that capability, we must develop relevant legal protections.

Working together, I think we can achieve strong privacy protection for personal health information. I look forward to the progression of our efforts toward that end.

Mr. CONDIT. Thank you, Tom. Do you have a few minutes to spend with us this morning?

Mr. SAWYER. Whatever will suit your purposes, Mr. Chairman.

Mr. CONDIT. I am going to turn to Mr. Thomas for any opening statement he would like to make.

Mr. THOMAS. Thank you, Mr. Chairman. I will submit it for the record. Just let me say I appreciate you having the hearing and I appreciate your being here. I think this is a tough issue. I think we have had some really good witnesses.

I hope that we might ask ourselves if the problems are due to a lack of regulations or, in fact, whether it is a violation of ethics currently in place. If it is the latter, then we should avoid issuing a whole new set of regulations for providers and, instead, look at solutions of other kinds.

It is difficult. As the President has proposed a national information system with regional data centers, it becomes more important that we train and educate consumers and I think that your proposition, Tom, will help do that.

There is a great deal of evidence that the government is incapable of collecting information very efficiently and, indeed, you might even question how much information the government should collect. There is that ongoing question, certainly within the Census Bureau.

The National Practitioner Data Bank is an example that has not been exactly perfect. It has designed to help hospitals access information about physicians but it had trouble with backlogs and has become the object of several investigatory reports.

It is a tough one and I hope we do not overindulge ourselves in this question of information on a national level, regarding everyone in this country. In any event I appreciate you having these hearings and I look forward to the rest of the witnesses, and thank you, Tom.

[The prepared statements of Mr. Thomas and Mr. Owens follow:]

Congress of the United States
House of Representatives
Washington, DC 20515-5001

OPENING STATEMENT

"FAIR HEALTH INFORMATION PRACTICES ACT"

May 5, 1994
2247 Rayburn House Office Building

Thank you, Mr. Chairman, for calling today's hearing. It is the last in a series of hearings the Subcommittee has held to review H.R. 4077, the "Fair Health Information Practices Act." The witnesses have been particularly helpful in their frank assessment of the Act and its affects on sensitive health care information.

As Congress reforms our health care system, the time is ripe to improve privacy protection standards. However, I would request that as we hear the recommendations from our final set of witnesses, that you ask yourself if a breach is due to a lack of regulations or a violation of ethics currently in place. If it's the later, then we should avoid issuing a whole new set of regulations for providers. And instead, look at the best solutions for training employees on the sanctity of individual medical information. We must also look at ways to educate patients on their right to request and amend information that has been incorrectly recorded about them.

Now that the president has proposed implementing a national information system with regional data centers, it will become even more vital to properly train and educate providers and consumers. Representative Thomas Sawyer will testify today on how we can best accomplish this task through the private sector.

Rarely is the federal government capable of collecting information efficiently. The National Practitioner Data Bank is a perfect example. This system was designed to help hospitals access information about physicians but it is plagued with backlogs and has become the object of several investigative reports. I cannot imagine how the administration thinks it can collect health care information cost-effectively for every single American -- a far cry from its "Reinventing Government" proposal.

The truth is, reforming health care so a family of four can purchase a basic insurance policy, does not require complex health alliances, regional data centers and national health boards. It requires simple, practical changes. And, if Congress does not refocus its objectives, this country will not be able to afford health care reform.

Mr. Chairman, I would appreciate you keeping these thoughts in mind as you make revisions to H.R. 4077. We need to make sure the legislation is practical and affordable for all to use. Thank you again for holding today's hearing.

OPENING STATEMENT OF CONGRESSMAN MAJOR R. OWENS
BEFORE THE SUBCOMMITTEE ON
INFORMATION, JUSTICE, TRANSPORTATION AND AGRICULTURE
May 5, 1994

I would like to thank Chairman Condit for holding hearings on this important issue. Each of us assumes that our medical records will be private, and that if they are not, we may sue the violator. This, however, is not always the case. There are significant gaps in privacy protection.

First, the current privacy laws only cover a small portion of the individuals with access to our medical records. Insurance companies and law enforcement officials, for instance, are not restricted in their use of medical information, and are allowed to use medical information in any capacity.

Second, there is no uniformity among privacy laws. They vary from state to state, and the level of confidentiality depends on the type of health information. New York and California have very strong HIV confidentiality laws. Other states have strict alcohol and drug confidentiality laws. What's protected in some states may not be protected in others.

A third gap in privacy protection arises when, health care providers, nurses, and their assistants are unclear as to their responsibilities to protect health information. In fact, many patients are unaware that by authorizing a provider to disclose medical information, they allow the doctor to disclose their entire medical record.

H.R. 4077 would fill in these gaps and give patients the privacy protection they deserve. The bill establishes uniform, comprehensive, federal guidelines that would govern the use and disclosure of all health records. It also outlines the responsibilities of each health care worker to protect a patient's privacy and defines how each may disclose the records. Finally, the bill establishes a patients' "bill of rights": the right to access their records; the right to make corrections to their records; and the right to seek retribution when their privacy is violated.

While I feel this is a good bill, I do have a couple of concerns. The first is the burden placed on patients to know and understand when they must prohibit the disclosure of some medical information in advance. In some cases, doctors have the authority to disclose information without the patient's knowledge or consent; in other cases, the doctors need a patient's written or oral consent. Keeping the various instances when an authorization is necessary may be very confusing for the patients. I am not confident that patients will understand that not all disclosures require their written consent.

I also am concerned about the federal pre-emption of state laws. Some states have very strong confidentiality laws that must not be weakened by this Act. My state of New York has strict privacy laws with respect to HIV confidentiality. I do not want to see these laws weakened, or any group of people lose the privacy protections they have now. I know advocates in the substance abuse community are concerned about the pre-emption issue as well. While I understand that having one clearly stated law governing the maintenance and transmission of health information reduces the paperwork burden, we as legislators should not forget that we are here to protect the privacy of individually-identifiable medical records. I particularly am interested in what Susan Jacobs from the Legal Action Center in New York has to say on the pre-emption issue.

I look forward to this morning's hearing in the hope that our witnesses will be able to shed some light on my concerns, as well as those of my colleagues on the Subcommittee.

Mr. CONDIT. Mr. Horn.

Mr. HORN. No questions, Mr. Chairman.

Mr. CONDIT. Tom, there has been some controversy about the using of health records in research without the consent of the patient. Do you support that kind of research, the use of statistical information? Do you have any feelings about that?

Mr. SAWYER. First of all, let me suggest that I do not think the use of data in any way that is less protected than what we have today, that uncertain patchwork of protections that exists largely on the State level, largely with regard to paper records, over which individuals have very little control today—I don't think that we ought to do less than that. I think there are opportunities to do more.

Let me just suggest that the notion of functional separation that you have provided in here—that is to say, the difference between records used for individually authorized applications for medical care and billing and so forth—and separating that from broader, aggregated uses is enormously important.

Where there are special cases, where research requires individual linkage, then it is enormously important that that not be identifiable individually.

Finally, the kind of work that is done regularly throughout this country, not only in censuses, but in the individual surveys that are conducted on economic activity throughout the country, the consent is achieved specifically with regard to the administration of that survey and is, in that context, meaningful.

Today, when health information is collected from individuals, the kind of blanket consent that is given by patients to hospitals, practitioners, insurers, physicians, others, is such a blanket signing away of consent that it is largely meaningless as a protection at best and I think at worst serves to mislead patients with regard to the kind of protections that they may think are or are not in place.

Mr. CONDIT. Can you give us your views on the use of the Social Security number as the health identifier?

Mr. SAWYER. I think it serves as a base from which to begin. I think it would probably not be wise to begin to set up a whole separate system of identifiers.

I think it also important to recognize that Social Security numbers not only do not have the full measure of security that I think many people would like to see but those numbers are, in fact, used over again. To have this be a unique identifier, I think, is fundamental to the system. Something like what other entities do in providing individual, secure identifiers can serve as a model.

Long distance and local telephone companies provide the use of your individual telephone number, which may or may not be more or less secure, depending on whether you are listed or not, and add to that a four-digit identifier that is easily remembered and would be difficult to match for anyone who is attempting to make use of your telephone number for long-distance identifier purposes. It is not perfect for those purposes.

However, a Social Security number, coupled with an individual and unique identifier, would, I think, go a long way toward making an affordable and secure system possible.

Mr. CONDIT. Mr. Thomas, do you have questions?

Mr. THOMAS. Just more of an observation. A lady in Greybull, WY would say, "What are you talking about?"

What are we seeking to develop here in terms of an information? Are we talking about research? Are we talking about backgrounds that move for treatment? Are we talking about who pays? Is the government going to be watching to see who pays? Are we talking about fraud? Are we talking about simply technology that has changed?

I am not sure, for many people, that we have really defined what it is we are requesting. What is the goal? What are we trying to do? How do you see that?

Mr. SAWYER. One of the things we are not trying to do is to have a government-collected data system. We are trying to put together a grid of carefully protected points of information—perhaps as many as 50 or more throughout the country—that rather than functioning like a national centralized data bank. If you are looking for an analogy, I would compare it more to the banking system and the disbursal of the Federal Reserve system, where, in fact, people do the same thing with their money that we are, in fact, asking them to do with health information.

The two things that people care most about are their health and their money. People actually go to banks, take money out of their pocket, give it over to a private-sector institution, and that money goes into an electronic network of asset transmission that people have confidence in because the protections and prohibitions are sound. It is not a government centralized repository.

Mr. THOMAS. That money is sort of fungible. You cannot identify the \$500 you put in the bank.

Mr. SAWYER. No, but the truth of the matter is, you sure want to make sure that that \$507.14 that you put in there never goes anywhere else and is always attributed to you and is secure and not accessible to anybody else and that it is private. That is what we do with a private system of information transfer.

That is what we are trying to create here under a system of government-directed laws, much as we write laws in other areas, but not to create a government-centered repository.

Mr. THOMAS. Good.

Mr. SAWYER. I think your concern is right on the money, so to speak. [Laughter.]

Mr. CONDIT. Little pun there.

Mr. SAWYER. Yes.

Mr. CONDIT. Thank you. Ms. Woolsey.

Ms. WOOLSEY. I have nothing, Mr. Chairman.

Mr. CONDIT. Mrs. Thurman.

Mrs. THURMAN. No, thank you, Mr. Chairman.

Mr. CONDIT. Mr. Horn.

Mr. HORN. No questions, Mr. Chairman.

Mr. CONDIT. Ms. Ros-Lehtinen, no questions?

Ms. ROS-LEHTINEN. No, Mr. Chairman.

Mr. CONDIT. Tom, thank you very much for your time. You have been very kind with it and we appreciate it.

Mr. SAWYER. Thank you, Mr. Chairman.

Mr. CONDIT. We will take the first and last panel. We have a practice, the committee, of swearing in all witnesses. If you will, remain standing, and raise your right hands.

[Witnesses sworn.]

Mr. CONDIT. Thank you very much. We do appreciate you being here this morning, and your input. We will start with Ms. Berenson.

**STATEMENT OF AIMEE R. BERENSON, LEGISLATIVE COUNSEL,
AIDS ACTION COUNCIL**

Ms. BERENSON. Thank you. I want to thank the members of the subcommittee and especially Chairman Condit for the strong leadership you have provided in bringing the critical issue of protecting the privacy of health information to the forefront and for giving AIDS Action the opportunity to testify here today.

The lack of any comprehensive Federal health information privacy law has meant that people living with HIV and AIDS and their advocates have been forced to fight the battle to protect their confidentiality State by State, government agency by government agency, and case by case. At the same time, we have battled highly politicized attempts to mandate disclosures of personal HIV-related health information.

Although people with HIV and AIDS continue the decade-long struggle to create confidentiality protections out of a hodgepodge of constitutional, State, regulatory, and common-law provisions, we still face the situation where the holes are too big, the ground beneath us is too unstable, and the costs are too great, to continue this fight as we have been. Congress must enact a comprehensive Federal health information privacy law.

We believe that the framework of H.R. 4077 can serve as the basis for creating such a law. I would like to set out what we believe are essential criteria for a Federal law and to briefly highlight the way we believe H.R. 4077 meets these criteria and where we believe clarifications or changes are needed.

Our first criterion is that any Federal law must provide a solid floor of protections which all States must meet and build upon as necessary. Providing a floor as opposed to a ceiling of protections is critically important to people with AIDS.

Over the course of this epidemic, enormous effort has gone into creating State laws that do provide protection for people and thus give them the confidence to come forward to be tested and treated for HIV. It is essential that we not undermine the progress that we have made in the last 12 years of this epidemic. Additionally, no matter how strong and comprehensive the law we create today may be, we must not preclude States from taking action in the future to provide greater confidentiality protections, if necessary.

The goal of providing a strong floor of protections can be met by explicitly providing that the Federal health law preempts any State law which fails to provide greater or equal protection. We believe H.R. 4077 is not sufficiently explicit in this regard, however, and should be amended accordingly.

Our second criterion is that any Federal law must place a legal duty to protect the confidentiality of personally identifiable health information on all persons and entities collecting or using such in-

formation. The current lack of comprehensive legal protection means that personal health information about one's HIV status may be protected if provided to a doctor for treatment but the same information, once provided to an insurer or employer, may not be protected.

H.R. 4077 makes significant progress toward providing comprehensive protection. However, we believe that further work needs to be done with regard to making the bill sufficiently comprehensive by, for example, extending the duty to protect information beyond just instances where that information is collected or used for treatment or payment.

Our third criterion is that any Federal law must ensure that the permissible uses and disclosures of personal health information are clearly defined and appropriately limited in scope. There must be firewalls between categories of authorized disclosures so that information provided for public health purposes, for example, cannot be disclosed or used for other purposes, even those that may be otherwise legally authorized.

This is particularly important for people with AIDS because the fear that personal health information provided for public health purposes could be accessed, disclosed, or misused has been an ongoing barrier to cooperation between people with AIDS and public health authorities.

Additionally, uses and disclosures must be limited to those that are compatible with or related to the purpose for which the information was originally obtained from the individual. It is imperative that the individual's expectation of privacy be respected, at least to the extent that she is assured that only disclosures of personal health information which are compatible with the purpose for which she gave the information in the first place are legally permitted.

Our fourth criterion is that any Federal law must provide individuals with sufficient notice and opportunity to limit access, use, and disclosure of public health information.

We are concerned with H.R. 4077 because it contains provisions authorizing disclosures unless there has been prior objection by the individual. Placing the burden on the individual to object prior to the disclosure without requiring the health information trustee to provide notice of the potential disclosure is grievously unfair.

For example, the next-of-kin provision in H.R. 4077 permits disclosure of protected health information to next of kin unless the individual has previously objected. This would allow potentially devastating disclosures to be made to an individual's family about her HIV status without ever asking the individual if she consents to such disclosure beforehand.

We believe the bill must be amended to provide greater formalization of the notice process to enable individuals to exercise what should be an inherent right to notice and an opportunity to object to infringements of their privacy.

Lastly, our fifth criterion is that any Federal law must provide strong legal remedies for violations. We strongly support the remedies included in H.R. 4077, which provides a private cause of action, the imposition of civil penalties for violations, and criminal

penalties for those who knowingly violate the law for profit or monetary gain.

We are concerned, however, with the bill's provision regarding the development of alternative dispute resolution methods. In the AIDS context, ADR has been used by defendants to drag cases out until the plaintiff dies.

ADR should only be used where all parties agree. Time limits must be placed on how long the process may take and the law must prohibit requiring any individual to waive their right to seek resolution of claims in court as a condition of getting treatment or reimbursement for care or services.

The enactment of a comprehensive Federal law that protects the privacy of all personal health information is critical to people living with AIDS and to all Americans. I applaud you for your commitment and your efforts. We look forward to working with you to realize our goals and I thank you for allowing me to testify before you today.

[The prepared statement of Ms. Berenson follows:]

**TESTIMONY OF AIMEE R. BERENSON, LEGISLATIVE COUNSEL
AIDS ACTION COUNCIL
BEFORE THE HOUSE GOVERNMENT OPERATIONS COMMITTEE
SUBCOMMITTEE ON INFORMATION, JUSTICE, TRANSPORTATION
& AGRICULTURE
May 5, 1994**

Good morning. My name is Aimee Berenson, and I am Legislative Counsel for AIDS Action Council, the Washington representative of over 1000 community organizations across the nation serving people with HIV/AIDS. I want to take this opportunity to thank the members of this Subcommittee, especially Congressman Condit, for the strong leadership you have provided in bringing the critical issue of protecting the privacy of health information to the forefront, and for giving AIDS Action the opportunity to testify here today about the importance of this issue for people living with HIV/AIDS across this nation.

Protecting the confidentiality of health information is not merely an academic concern for people living with HIV/AIDS. Tragically, the over 1.5 million Americans currently infected with HIV not only face a battle against the disease itself, but against the fear, prejudice, stigma and discrimination that have been the darkest companions of this AIDS epidemic. People living with HIV/AIDS have lost their jobs, their homes, and the companionship and support of their families, friends, co-workers, and communities as a result of their illness. Perhaps even more appalling is the fact that people living with this disease have found themselves discriminated against in the health care system itself -- by doctors, dentists and hospitals who refused to treat them, or by insurers who denied their claims or capped their benefits.

For people living with HIV/AIDS, maintaining confidentiality is essential to preventing discrimination. Studies have shown that the very fear of breach of confidentiality may deter people from being tested for HIV, and that people who suspect that they may be HIV-positive delay early detection and treatment to avoid the potential negative consequences which flow from confidentiality breaches.¹ Thus the lack of confidentiality may cause people to avoid early detection and treatment of their HIV disease, treatment which can greatly improve both the quality and duration of life. Others are frightened into obtaining medical care and services under assumed names to protect themselves, their families, and their friends from the potential consequences of breaches of confidentiality.

Sadly, the fears that cause people at risk of or infected with HIV to avoid the health care system are well-founded. The reported cases of breach of confidentiality of HIV-related health information (which probably reflect only the tip of the iceberg) are a distressing indicator of the potential magnitude of the problem. For example:

-- A New Jersey court found that a hospital's failure to limit access to an HIV-positive patient's medical records resulted in the ostracization of the patient and his wife in their community.²

-- A New York doctor was found to have violated that state's confidentiality law by

¹ American Bar Association AIDS Coordinating Committee, Issues Relating to AIDS and Health Care Reform, at 30-31 (July 1993).

² Behringer v. Medical Center, 249 N.J. Super. 597, 595 A. 2d 125 (N.J. Super. Ct. 1991).

providing copies of her patient's HIV-related medical records to a worker's compensation board without the patient's consent.³

-- A California patient alleged that his doctor violated the privacy clause of the state constitution by disclosing the patient's HIV status to others without the patient's consent.⁴

-- An HIV-infected hospital patient in Maryland sued after hospital personnel allegedly disclosed his HIV status to family and friends.⁵

-- A Pennsylvania woman alleged that a hospital improperly approved the release of false information that the woman had AIDS.⁶

The AIDS epidemic has highlighted the inadequacy of the current patchwork of existing state and federal confidentiality provisions. The lack of any federal health information privacy legislation has meant that people living with HIV/AIDS and their advocates have been forced to fight the battle to protect the confidentiality of their health information state by state, government agency by government agency, and case by case, struggling to make a patchwork of state laws that all too often provided little or no protections work. At the same time, we battle attempts to further stigmatize and discriminate against people with this disease by mandating disclosures of highly personal health information for political rather than public health purposes.

In some states, efforts to carve out strong HIV confidentiality protections have been fairly successful -- New York and California are notable examples. In other states, such as Illinois, for example, people living with HIV/AIDS have faced the chilling specter of highly politicized attempts to access legally protected information (namely information provided for public health surveillance purposes) in order to conduct witch hunts to ferret out HIV-infected individuals.

Protecting HIV-related health information has been further complicated by the fact that in many instances, health care information generally is not protected, and so the very fact that a certain individual's health record is confidential discloses the fact that the individual has HIV. In other instances, only certain aspects of health information are protected -- for example, the fact that an individual has tested positive for HIV may be protected information, but the information that the individual is getting a prescription filled for AZT is not. And in some instances,

³ Doe v. Roe, No. 92-1642 (N.Y. Sup. Ct., July 31, 1992).

⁴ Estate of Urbaniak v. Newton, 226 Cal.App.3d 1128, 277 Cal.Rptr. 354 (Cal. App. 1991).

⁵ Doe v. Shady Grove Adventist Hosp., 89 Md.App. 351, 598 A.2d 507 (Md. Ct. Spec. App. 1991).

⁶ Burton v. Yeager, Complaint No. 87-00287 (Pa. Ct. Common Pleas, filed 1987), reported in Lambda Legal Defense and Education Fund, AIDS Update, Aug. 1987.

confidentiality is protected only in the hospital or health care provider setting, so that when that confidential information is sent to an insurance company or social service provider, it is no longer protected. Thus, even in states that have HIV-related confidentiality protections, the extent of those protections may be limited.⁷ Computerization, needless to say, adds to the potential universe of people and entities who may have access to information, and further heightens the already-existing fears people have about potential breaches of confidentiality.

In developing state laws to protect the confidentiality of HIV-related information, AIDS advocates have focused on two areas: limiting the uses and disclosures of HIV-related information, and ensuring that individuals have control over, and thus confidence in, how personal health information will be used, by creating more genuine "informed consent" written authorization procedures.

Traditionally, the "informed consent" model of protecting health care information has not worked well, because in reality individuals have lacked the information necessary to enable them to truly give "informed" consent. Often individuals do not realize the actual universe of people and entities that have access to their personal health information, or understand that there are few limits on the uses or disclosures of information that those with access may make.

People with HIV/AIDS are usually aware that information of their HIV/AIDS status may be provided to public health departments for public health purposes, for example, and have fought (and continue to fight) hard to protect their confidentiality in that public health reporting process. Yet people living with HIV/AIDS, like most Americans, are much less likely to realize that within the physician's office, hospital, laboratory, or pharmacy, their personal health information may be accessed -- and potentially disclosed -- by anyone from nurses and technicians to orderlies and receptionists to billing departments. Currently, there may or may not be internal organizational policies limiting the extent of access to an individual's medical record, or limiting use and disclosure of information. Individuals rarely know what the case is in a given setting.

Moreover, individuals are routinely required to sign forms authorizing the health care provider to disclose information to insurers. People generally don't realize that this authorization gives the insurer access to their entire medical record; even if they did, most are not in a position to limit such access. A refusal to sign the authorization means the provider cannot be reimbursed, and thus is unlikely to provide treatment or services unless the individual has the ability to pay the costs out-of-pocket, and usually on the spot.

⁷ For example, in the Urbaniak case mentioned earlier, a California Court of Appeal, while sustaining the plaintiff's state constitutional privacy claim, held that the state's HIV confidentiality law only applies to disclosure of the actual record of an HIV blood test result, and not to disclosures of information obtained from other sources regarding an individual's HIV status. Urbaniak, 277 Cal. Rptr. at 362.

Again, the insurers' access means that many people, from claims processors to utilization reviewers to accounting department personnel, have access to the individual's medical record. Even employers have access to information in that record, if for example the employer is self-insured, or if a third-party insurer is providing information about claims to justify premium hikes based on utilization costs, pre-existing conditions, etc.

This poses a devastating dilemma for people living with HIV/AIDS, since they are forced to disclose their illness in order to get insurance companies and medical professionals to provide care, yet may in fact find themselves denied care, legally or otherwise, on the basis of the very information they must disclose to get care.

In essence, although people with HIV/AIDS continue the decade-long struggle to create confidentiality protections out of a hodge-podge of constitutional, state, regulatory, and common-law provisions, we still face a situation where the holes are too big, the ground beneath us too unstable, and the costs too great to continue to fight this fight as we have been. Now, as this Congress and this country engage in the monumental task of reforming a health care system that has insured the healthy and failed the sick and the poor, it is also time to address the failure of our health care system to respect and protect the dignity and privacy of those it is supposed to serve.

The Need For A Comprehensive Federal Health Information Privacy Law

The problems faced by people living with HIV/AIDS, and all Americans, as a result of the lack of privacy protections for personally identifiable health information can only be addressed through the enactment of a comprehensive federal health information privacy law. We believe that in order for such a law to be effective, it must meet the following essential criteria:

- Provides a strong, uniform "floor" of protection for all personally identifiable health information.
- Places a legal duty on all individuals and entities which create, collect, or use personally identifiable health information to protect the confidentiality of that information.
- Clearly defines permissible uses and disclosures of information and builds "firewalls" to prevent the use or disclosure of information for unauthorized or incompatible purposes.
- Provides individuals with sufficient notice and opportunity to limit access, use and disclosure of personally identifiable health information.
- Provides strong, effective legal remedies and sanctions for violations of the law.

We believe that the framework of H.R. 4077 can serve as the basis for creating a federal law that meets these essential criteria. I would like to take this opportunity today to outline for you where we believe H.R. 4077 "works" and where we believe clarifications or changes are needed.

Providing a strong, uniform "floor" of protection for all personally identifiable health information

The most important thing Congress can do to restore the loss of dignity, privacy, and trust to our health care system for people living with HIV/AIDS is to enact a comprehensive federal law that safeguards the confidentiality of all personal health information. Such a law should provide a solid floor of protections, which all states must meet and build upon as necessary.

This issue of providing a floor, as opposed to a ceiling, of protections is critically important to people living with HIV/AIDS. As I discussed earlier, the lack of confidentiality protection has had a profound effect on the willingness and ability of people to come forward to be tested and treated for HIV. Over the course of this epidemic, enormous effort has gone into creating state laws that do provide protection for people and thus give them the confidence to come forward to be tested and treated for HIV. It is essential that we not undermine the progress, however limited it may be, that we have made in the last 12 years of this epidemic.

In fact, the very existence of the AIDS epidemic demonstrates the wisdom of setting a strong floor of federal protections, rather than a ceiling. If this hearing had been held in 1979, none of us would have foreseen the devastating epidemic that is now upon us, or understood in quite so profound a manner, perhaps, how the lack of strong, uniform health information privacy protections would affect so many Americans in so many ways as it has in the course of this epidemic. We must not shut our eyes to the frightening but real possibilities that future events may similarly affect us. No matter how strong and comprehensive the law we create today may be, we must not preclude states from taking action in the future to provide greater confidentiality protections if necessary. In the 12 years of this epidemic alone, no federal health information privacy law has been enacted. We cannot risk that some state needing to provide greater protections than we develop in this law in order to protect its citizens in some future situation will be forced to wait for Congress to act.

The goal of providing a strong floor of protections can be met by explicitly providing that the federal health information privacy law preempts any state law which fails to provide greater or equal protection of health information than the federal law provides. We believe that H.R. 4077 is not sufficiently explicit in this regard, however, and should be amended accordingly.

Additionally, because of the intrinsic link between breaches of confidentiality and discrimination, we believe that any federal health information privacy law should include a provision explicitly stating that nothing in the federal law shall be construed to deny, impair, or otherwise adversely affect a right or remedy otherwise available under any civil rights law. H.R. 4077 does not contain such a provision, and should be amended accordingly.

Placing a legal duty on all individuals and entities which create, collect, or use personally identifiable health information to protect the confidentiality of that information

Any federal health information privacy law must protect all personally identifiable health information, regardless of whether such information is collected or used by health care providers, insurance companies, employers, researchers, marketers, government agencies, laboratories, or any other institutional entity. Providing comprehensive protection is critical to people living with HIV/AIDS. The current lack of comprehensive protection means that personally identifiable health information about one's HIV status may be protected if provided to a doctor for treatment, but the exact same information, once provided to an insurer or employer, may not be protected.

H.R. 4077 makes significant progress towards providing comprehensive protection of health information. First, the bill establishes a comprehensive definition of protected personally identifiable health information.⁸ Second, H.R. 4077 sets out categories defining "health information trustees"⁹ who have a duty to "maintain reasonable and appropriate administrative, technical, and physical safeguards" to ensure the confidentiality of health information, and to protect against anticipated threats or hazards to the security of that information, including protection against improper uses or unauthorized disclosures.¹⁰

Particularly important for people with HIV/AIDS is the separation of public health authorities and public health uses of information from other types of health information possessors and users, such as health care providers, insurance companies, and hospitals. In fact, the majority of HIV-related confidentiality concerns have centered on the provision of personal health information for public health purposes, and around the fear that such information could be accessed, disclosed, or misused because there are insufficiently strong "firewalls" between public health information collection and other data collection and uses. We are pleased that H.R. 4077 recognizes these concerns by creating a separate category of "public health trustees", although we believe that several technical amendments to these provisions are needed.¹¹

⁸ See Section 3(a)(3).

⁹ See Section 3(b).

¹⁰ See Section 115.

¹¹ Section 3(b)(7) of the bill defines "public health authority"; Section 3(b)(8) defines "public health trustee". Only a "public health authority" or an officer or employee of such should be considered a "public health trustee"; therefore, the bill should be amended to strike the improper inclusion of "health researcher" in the "public health trustee" category. Additionally, to more accurately describe the types of public health activities undertaken by public health authorities, Section 102(3)(a), which is overly vague, should be stricken, and Sections 3(b)(7) and 125, which list legally authorized public health activities, should be amended to add "public health interventions".

Clearly limiting the permissible uses and disclosures of information and creating "firewalls" to ensure that information collected and used for specific purposes cannot be used for other, incompatible purposes

Obviously, defining the universe of people and entities that have a duty to protect personally identifiable health information is critical. Equally critical, however, is ensuring that the permissible uses and disclosures of such information are clearly defined and appropriately limited.

As the cases described earlier in my testimony illustrate, people living with HIV/AIDS have faced problems resulting from two kinds of unauthorized disclosures: disclosures to persons within an institution or office that possessed personally identifiable health information, and disclosures of that information to persons or entities outside of the institution or office.

In order to protect information within an institution or office, the federal health information privacy law must first place a duty to protect information on all people who act, in whole or part, in the capacity of officers or employees of an institution or office. Second, the federal law must limit the use or disclosure of information within an institution or office to those uses or disclosures that are compatible with or directly related to the purpose for which the information was collected or obtained. Such internal disclosures of personally identifiable health information must also be limited to the minimum amount of information necessary to accomplish the purpose for which the information is being disclosed.

We believe that H.R. 4077 does provide a framework of protections with regard to internal uses and disclosures of information. However, the bill as currently written leaves a major gap in protection that must be addressed. As currently written, the bill seems to limit the duty of health information trustees to protect personally identifiable health information to instances where such information was collected or used for purposes of treatment or payment. This limitation means that the very same information collected or used by the very same health trustee for purposes of obtaining insurance or employment, for example, would not be protected. We believe the bill must be amended to clarify that personally identifiable health information collected or used by a health information trustee is protected, regardless of whether such information is collected or used for treatment or payment purposes or for purposes such as obtaining insurance or employment. This is particularly important for people living with HIV/AIDS, given the intrinsic link between improper use and disclosure of confidential health information and discriminatory practices by employers and insurance companies.

We do not believe that H.R. 4077 provides sufficient protections with regard to external disclosures, namely disclosures of personally identifiable health information to persons or entities outside of the institution or office which possesses the information. While H.R. 4077 limits such disclosures to those that are "specifically authorized" in the bill, and "where practicable", to the minimum amount of information necessary to accomplish the purpose for which the information

is used or disclosed¹², the bill does not limit external disclosures to those disclosures that are compatible with or related to the purpose for which the information was originally obtained. Given that external disclosures pose such a great risk of harm to people living with HIV/AIDS, this is not acceptable.

We believe that the overall restrictions on external disclosures should be at least as strong as the restrictions on internal uses of personally identifiable health information. In other words, we believe external disclosures should only be permitted where specifically authorized by the federal law and where such disclosure is compatible with or related to the purpose for which the information was originally collected or obtained.

This change provides consistency, but more importantly, gives greater deference to the privacy expectations of the individual. Particularly where the law is not modeled on the traditional "informed consent" paradigm, it is important that the individual's expectation of privacy be respected, at least to the extent that he or she is assured that only disclosures of personally identifiable health information which are compatible with or related to the purpose for which the individual gave the information in the first place are legally permitted.

With regard to specifically authorized external disclosures, I want to reiterate our support for the creation of "firewalls" between disclosures for legally authorized public health activities and other types of disclosures. These firewalls are essential to protecting people living with HIV/AIDS and to maintaining confidence in the public health system.

One other authorized disclosure provision which I want to mention regards disclosures of information in emergency circumstances. While we think it is essential to have such a provision, we feel the provision as currently written fails to clearly define what an emergency is or who may be given protected information in such an emergency.¹³ We believe that the emergency circumstances provision should only permit a health information trustee to disclose protected information to an individual in emergency circumstances when such disclosure is immediately necessary to preserve or protect the health or safety of that individual.

Providing individuals with sufficient notice and opportunity to limit access, use and disclosure of personally identifiable health information

While we understand that H.R. 4077 rejects the "informed consent" paradigm, and while we agree that "informed consent" is usually neither, we still believe that the individual has the right to meaningful notice of what uses and disclosures of personally identifiable health information are legally permitted, in order to provide the individual with the opportunity to object to such uses or disclosures.

¹² See Section 121.

¹³ See Section 126.

The bill provides essential protections in this regard for written authorizations, but these protections will only apply to a fairly limited set of circumstances.¹⁴ The only guaranteed notice that individuals will receive regarding the use and disclosure of personally identifiable health information will be the Notice of Fair Information Practices described in Section 113 of the bill. As currently drafted, however, the bill does not require a health information trustee to inform an individual that they should read the Notice and indicate if they wish to object to a particular use or disclosure described therein.

This is a particularly problematic flaw in H.R. 4077, because the bill contains several provisions authorizing disclosures unless there has been prior objection by the individual to such disclosure. Placing the burden on the individual to object prior to the disclosure, without requiring the health information trustee to provide notice of the potential disclosure, is grievously unfair. If the health information trustee does not notify the individual of the potential disclosure and inform him or her of the right to object, there is really no meaningful opportunity for the individual to exercise that right.

This problem is most obvious in the bill's provision regarding disclosures to "next of kin". This provision permits disclosure of protected health information consistent with "accepted medical practice" to next of kin regarding the "on-going provision of health care" unless the individual has previously objected to such disclosure.¹⁵ This language is much too broad, and would allow potentially devastating disclosures to be made to an individual's family about his or her HIV-status, without asking the individual if he or she consents to such disclosures in advance. We fear that unless this prior objection problem is addressed in the legislation, people living with HIV/AIDS may be seriously harmed.

We believe that the overall problems regarding notice and opportunity could be addressed if the bill were amended to provide that a health care trustee who does not obtain specific written authorization must provide a copy of the Notice of Fair Information Practices to each individual, along with a statement clearly telling the individual that he/she has the right to object in writing to any of those practices at any time. The bill should also require that a notation be made that the individual was given the form, told to read it, and informed of his/her right to object.

Without creating some greater formalization of the notice procedures, there is no way for an individual to exercise what should be an inherent opportunity to object to the infringement of his or her privacy. Creating mechanisms such as those outlined above will not only address the prior objections burden problem, but will also ensure that individuals are able to meaningfully exercise their right to control the use and disclosure of personally identifiable health information.

¹⁴ See Section 122.

¹⁵ See Section 124(a).

Providing strong legal remedies for violations

A law may provide the most comprehensive privacy protections imaginable, but unless there are strong and effective provisions to enforce those protections, the law is meaningless. Since the beginning of the AIDS epidemic, the struggle to fight the disease has been complicated by attempts to fight people with HIV/AIDS. Too often, the policies and practices of governments and institutions have stigmatized people with HIV/AIDS and condoned, implicitly or explicitly, the denial not only of essentials like jobs, housing, health care and insurance coverage, but of fundamental rights to privacy, dignity, and equality as Americans.

The creation of a federal privacy law for personally identifiable health information presents the promise of a fundamental change in one aspect of the lives of people infected with and affected by HIV that may have far-reaching implications for addressing many of the other challenges they face. This promise, however, can only be realized if strong, effective, and accessible enforcement mechanisms are available to deal with those who violate the law.

Therefore, we believe that any federal health care information privacy law must create a private cause of action to redress violations. Individuals who have been harmed as a result of the intentional or negligent failure of an individual or entity to comply with the duties and obligations set out in the law must have the right to seek redress in the courts. The penalties for such violations must be significant enough to serve as a true deterrent, particularly in light of the financial incentives that may exist to violate an individual's right to privacy and confidentiality. Thus individuals should have the right to actual damages, punitive damages, and attorney's fees.

Additionally, because of the strong public interest in protecting health information and ensuring compliance with the law, the Secretary of Health and Human Services should have the power to impose civil penalties on those individuals or entities that fail to comply with the provisions of the law.

Lastly, given what may be substantial financial incentives to violate the law, we believe there must be criminal penalties for those who knowingly violate the law for profit or monetary gain.

H.R. 4077 provides all of these important enforcement mechanisms, and we applaud the drafters of the bill for recognizing the importance of strong and effective enforcement provisions to ensuring that the law provides more than just paper protections.¹⁶

We are concerned, however, with the provisions regarding the development of Alternative Dispute Resolution (ADR) methods by the Secretary of Health and Human Services.¹⁷ While

¹⁶ See Subtitle E.

¹⁷ See Section 163.

there is nothing inherent in the theory of ADR that we find problematic, we have experienced the reality of ADR as a tool used to delay resolution of claims and to increase costs to the plaintiff. In the context of AIDS-related discrimination complaints, for example, ADR has been used by employers, insurers, and health care entities to drag cases out until the plaintiff dies.

Our experience demonstrates that ADR methods should only be used where all parties to the dispute agree; that time limits must be placed (through legislation or regulation) on how long the ADR process may take; and that the law must prohibit requiring any individual to waive any rights to seek resolution of claims in court as a condition of getting treatment or reimbursement for care or services.

Conclusion

The enactment of a comprehensive federal law that protects the privacy of all personally identifiable health information is critical, to people living with HIV/AIDS and all Americans. The advent of health care reform has certainly brought the need for such a law to the forefront, but the importance of this issue itself demands action. People living with HIV/AIDS, perhaps more than any other group of Americans, have suffered the terrible consequences of the lack of a strong, comprehensive, federally-mandated floor of protection for personally identifiable health information. Many people with AIDS have lost their lives because of this disease; but many have lost their jobs, their homes, their insurance coverage, their privacy -- not because of disease, but because of fear, hate, prejudice, and discrimination.

Congress has the power -- and the moral imperative -- to enact federal legislation to protect the privacy of personal health information. Such legislation will move us that much closer toward ending the intolerable epidemic of discrimination that has tragically accompanied the AIDS epidemic in this country.

On behalf of AIDS Action and people living with HIV/AIDS across this nation, I applaud you for your commitment and your efforts. We look forward to working with you to realize our goals, and I thank you for allowing me to testify before you today.

Mr. CONDIT. We appreciate your being here very much.

Mr. HORN. Mr. Chairman, I have to testify before the Appropriations Committee. May I ask one question?

Mr. CONDIT. Absolutely.

Mr. HORN. I hope to be back before you all are done. I would just like to know the policy of your group on just one question.

I agree with you on the next of kin, unless the next of kin has a sexual relationship with the individual that has AIDS. Now, what is the policy of you and the groups you represent in terms of notification? Let us say, it could be blood transferred. We do not know what it is.

I just went with a Federal judge to have an AIDS victim from blood transfusion become an American citizen. He was Canadian. He was disowned by his family and so forth and so on, so I understand the next of kin.

However, when it comes to a relationship that would normally be expected to be sexual, such as a spouse of one sort of another, living with that individual, what is your feeling on notification then?

Ms. BERENSON. I think that issue is addressed through the public health activities. Currently, public health departments have partner notification processes by which the sexual contacts of a person who is HIV-positive can be notified and, additionally, that person—the person with HIV—can be counseled about how to notify their sexual contacts personally.

There is nothing, to my understanding, in H.R. 4077, that would prohibit or change that currently existing system.

Mr. HORN. You are saying that an individual cannot deny that notification for one reason or another?

Ms. BERENSON. I think that if the issue is around whether someone other than a public health authority can contact the sexual partner of someone with HIV, right now that is an issue that is dealt with in a number of State laws and generally it is an issue of when is it appropriate for a physician to violate a particular patient's confidentiality. We do not believe that there is any particular reason to think that H.R. 4077 would make that situation worse than it is now, and we believe that, through the public health provisions, we are addressing that issue.

Mr. HORN. My only problem would be I would hate to see a variation in State law where the individual who is the sexual partner would not be notified.

Ms. BERENSON. I do not believe that there is any State that does not have provisions for providing notification.

Mr. HORN. I remember a few years ago—and I have not kept track of this recently—when I was chairman of the National Institute of Corrections, we faced this problem with, when an individual secures AIDS in prison, do you notify the spouse of that individual when they leave prison and what is the responsibility, if any, of the Federal Government if you do not notify?

Yet, I believe California had a law where that was very questionable if you did notify. I am not sure where that is now. Maybe you know.

That is the area that worries me because this is not any transmittable disease. This is the one that results in death, at this point.

Ms. BERENSON. I would certainly be more than happy to try to get that information for you about what specific States do in that regard.

Mr. HORN. Yes. I think, whatever it is, we need to clarify our position on at least that one point. I think it would be irresponsible not to clarify it.

I appreciate your testimony and I hope to be back shortly.

Ms. BERENSON. Thank you.

Mr. CONDIT. Thank you, Mr. Horn. Does any other member have a followup to Mr. Horn's question?

[No response.]

Mr. CONDIT. Ms. Jacobs.

STATEMENT OF SUSAN L. JACOBS, STAFF ATTORNEY, LEGAL ACTION CENTER, NEW YORK, NY

Ms. JACOBS. Thank you, Mr. Chairman. I would like to thank the chairman and the subcommittee for the opportunity to testify today on behalf of the Legal Action Center.

The Legal Action Center is the only organization in the United States specializing in policy and legal issues in the intersecting areas of drug and alcohol abuse and AIDS. We have worked for over two decades with individuals affected with these diseases and with the public and private institutions that provide them with treatment, health care, and other social services.

One of our principal areas of concentration is on confidentiality of patient records and we have also been recently deeply involved in national health care reform, particularly as it affects persons receiving treatment for alcohol and substance abuse and AIDS.

I want to outline briefly the privacy considerations of a the unique population of users of the health care system. That is, individuals receiving treatment for alcohol and drug abuse. I want to also summarize the Federal protections now afforded these clients and mention how the Fair Health Information Practices Act, H.R. 4077, would change this protection and what we suggest be done about that impact.

I would like to begin by expressing my deep appreciation to the subcommittee and especially Mr. Gellman, chief counsel, for the concern they have shown about the impact of privacy legislation on the lives of our clients.

We further agree with the subcommittee that privacy of health care records ought to be protected by Federal legislation. However, the records of our clients in specialized alcohol and drug treatment programs are already protected by practical and effective Federal legislation and we respectfully submit to you that these protections ought to be left in place and not preempted by the act.

These laws and regulations are stronger and more specifically targeted for our population, essentially, than the privacy protection proposed by the act. The preservation of these protections is crucial to the success of alcohol and drug treatment programs nationally.

The existing Federal confidentiality laws for alcohol and drug treatment records were passed by Congress in the early 1970's. They narrowly define the circumstances in which the records of patients in federally assisted substance abuse treatment programs may be disclosed.

The legislative history of the statute and regulations—which I will not go into detail about now but are reflected in my statement—express your strong recognition of the difficulty of getting people into treatment when they have drug and alcohol problems and retaining them in treatment.

Obviously, the problems of such abuse reach deeply into all classes and all races and, unfortunately, these problems continue to be stigmatizing even after people are in health care for these problems and even years after successful recovery, so a wrongful disclosure can end a career, destroy a marriage, or devastate a friendship.

Specialized alcohol and drug treatment programs therefore may make no disclosures at all which reveal that an individual person is receiving diagnosis, treatment, or referral except, obviously, under certain very delineated circumstances. These disclosures, in our experience, allow every reasonable request to be fit but they do so in a way that is quite different, in some regard, from the Fair Health Information Practices Act, and I want to mention three areas where that is significantly different.

The first is in the area of investigations of suspected or actual criminal activity. Because addiction involves the illegal use of drugs, persons seeking treatment for addiction are very vulnerable, especially when they first enter treatment and, in fact, are making the decision to come into treatment and, also, in later stages, because of their past criminal activity.

Under the existing Federal law, an investigative law enforcement or prosecutorial agency must obtain a court order to obtain information from a drug and alcohol treatment program even if law enforcement officials have a search warrant. This issue is very vital to drug and alcohol treatment programs, yet the act that you have written does not provide the protection of an extra court review or court order in these circumstances.

As a result, alcohol and drug treatment programs would have to disclose identity of clients that they do not need to disclose now, not only if they were the subject of an investigation but also if they were a witness or a figure in an inquiry conducted by law enforcement. Unfortunately, because of the activities people had formerly been engaged in before they come into treatment, they do wind up being involved in or asked to be witnesses for many of these kinds of inquiries.

The second area in which the act differs from the current protection is in disclosures to family and next of kin. Federal alcohol and drug confidentiality law provides crucial protections for clients dealing with families because alcohol and drug abuse can be so intricately involved in family dynamics.

These protections have been especially important, for instance, for women entering treatment, because they are often in relationships with men who encourage their use of drugs or alcohol and disapprove, sometimes violently, of their coming into treatment. The written consent process which is now available in the drug-alcohol law and is not required under the act is crucial to keep clients and patients aware of which family members might get information and which families will not.

For instance, section 124 of the act allows a health information trustee to disclose information, protected information, to the cli-

ent's next of kin, without specific consent of the individual. The section does prohibit the disclosure if the individual previously objected but that is far less protective than the affirmative standard that we have now.

The last area I want to raise is in disclosure to employers. Under Federal alcohol and drug confidentiality law, again, other than by consent, information identifying an employee as being in treatment would virtually never be given to an employer. Under the act, health information trustees and payers exchange information without written consent of the client, in some instances.

In the case where treatment is paid for directly by employers, there is not any provision comparable to the consent form that we now have for narrowing that information.

Because of the stigma attached to alcohol and drug dependence, many persons with this illness are subject to termination by employers and, unfortunately, if the employer decides that the patient should be fired for being a drug user—although we expect that that does not happen often—the ADA, the Americans With Disabilities Act, would, unfortunately, not protect that client who may, in fact, be a current user of illegal drugs—again, the person who is very vulnerable as they come into treatment and may still be having trouble stopping use.

Finally, we are also very concerned about the confidentiality of information concerning people with HIV and AIDS since a great number of the clients of alcohol and drug treatment programs are at high risk for or have these infections. We support the concerns about preemption of State HIV confidentiality law expressed by organizations such as AIDS Action Council in their testimony today.

Finally, we appreciate the importance the subcommittee places on the need for Federal privacy legislation in health care reform. Our experience in serving a unique population and their clients is that confidentiality protections in 42 U.S.C. 290dd and ee-3 are uniquely tailored for their needs. To continue national efforts at controlling alcohol and drug dependence, we believe the statute and implementing regulations must remain in effect and not be preempted by the act.

Thank you for your attention.

[The prepared statement of Ms. Jacobs follows:]



153 Waverly Place • New York, NY 10014 • (212) 243-1313 • FAX: (212) 875-0286

Board of Directors

Arthur L. Liman,
Chairman
Peter Barton Hutt,
Vice Chairman
R. Palmer Baker, Jr.
Eric D. Raiber
Elizabeth Bartholet
Patrick R. Cowlishaw
Haiton L. Dalton
Diana R. Gordon
Neal J. Hurwitz
Barbara A. Margolis
Daniel K. Meyers
Alice E. Mayhew
Michael Mellinger
Mark C. Morris
Robert G. Newman
June E. Osborn
Richard Pruss
Alan Rosenfeld
Ian Schragar
Jane Velez

Staff

Paul N. Samuels
Director/President
Catherine H. D'Neil
Executive Vice President
and Director of HIV/AIDS
Projects
Sally Friedman
Susan Galbraith
Co-Director
of National Policy
Susan L. Jacobs
Felix Lopez
Anita R. Marlon
Ellen M. Weber
Co-Director
of National Policy
Jamie Johnson
Manager of Administration
and Finance
Tony D. Ross
Project Director

Policy Associates

Robb Cowe
Joseph M. Frisno

Paralegals

Hetty Dekker
Roberta A. Meyers

Office Manager

Gladys Peoples

TESTIMONY OF THE LEGAL ACTION CENTER

Before The Subcommittee Of
The Committee On Government Operations On The
H.R. 4077, The Fair Health Information Practices Act of 1994

May 5, 1994

Presented by

Susan L. Jacobs
Staff Attorney

Introduction:

I would like to thank the Chairman and subcommittee for the opportunity to testify today on behalf of the Legal Action Center (LAC). LAC is the only organization in the United States specializing in policy and legal issues in the intersecting areas of drug and alcohol abuse and AIDS. We have worked for over two decades with individuals affected by these diseases and with the public and private institutions that provide them with treatment, health care and other social services.

One of our principal areas of specialization is the confidentiality of patient records. Center staff worked closely with the Department of Health and Human Services on revising the federal confidentiality regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR Part 2) and have written two books and numerous articles about these topics. We have lectured on these issues in more than 40 states. By contract, we provide assistance on confidentiality problems to thousands of alcohol and drug programs in 27 states. LAC has also been deeply involved in national health care reform, particularly as it affects persons receiving treatment for alcohol and substance abuse and AIDS.

In our testimony we will outline the privacy considerations of a unique population of users of the health care system — individuals receiving treatment for alcohol and other drug abuse. We also summarize the federal protections now afforded these clients, how the Fair Information Practices Act of 1994 (the

Act) would change this protection and what we suggest be done about that impact.

We would like to begin by expressing our deep appreciation to the subcommittee and especially Mr. Gellman, chief counsel, for the concern they have shown about the impact of privacy legislation on the lives of our clients. LAC realizes that the streamlining of information transfer would be a beneficial component of any health care reform proposal, and that streamlining efforts are aided by rapid technological advances. We applaud the subcommittee for its recognition that these changes and technological advances require government to balance the needs of the health care system for the flow of information with the privacy rights of individuals with regard to their health care records. We further agree with the subcommittee that the privacy of health care records ought to be protected by federal legislation.

However, the records of our clients in specialized alcohol and drug treatment are already protected by practical and effective federal legislation, and we respectfully submit that those protections ought to be left in place and not preempted by the Act. As we will discuss, the federal laws and regulations governing the confidentiality of the records of persons in specialized alcohol and drug treatment programs are stronger and more specifically targeted than the privacy protection proposed under the Act, and the preservation of these protections is crucial to the success of alcohol and drug treatment programs nationally.

It is estimated that approximately three million people annually receive treatment for alcohol and drug dependence nationally.¹ Virtually all of these people are served in specialized alcohol and other drug treatment programs whose patient records are covered by 42 USC §§ 290—dd-3, ee—3. As written, the Federal Fair Information Practices Act would preempt this statute. For the reasons outlined below, it is our strong belief that the Act should be amended so that this law is not preempted. We make this recommendation with the awareness that when introducing the Act, Chairman Condit acknowledged that preemption is an area in which more work needs to be done and that in order to accomplish the bill's major goals, "we may not have to preempt every law".

**The Existing Federal Confidentiality Laws for Alcohol
and Drug Records**

Two statutes passed by Congress in the early 1970's, 42 USC §§ 290dd—3 and ee—3, narrowly define the circumstances in which the records of patients in federally assisted substance abuse treatment programs may be disclosed. Both statutes delegated rule—making responsibility to the former Department of Health, Education, and Welfare (HEW), now HHS, and in 1975,

¹ "Healthcare Reform and Substance Abuse Treatment: The cost of Financing Under Alternative Approaches," Lewin-VHI, Inc., Jan. 19, 1994.

HEW issued an exhaustive set of regulations entitled "Confidentiality of Alcohol and Drug Abuse Patient Records" (hereinafter "the regulations") 42 CFR Part 2. These regulations, revised once in 1987, supersede any state or local law less protective of the confidentiality of patient records. For all practical purposes these regulations constitute the universe of legal requirements in this area. The legislative history of the statute and regulations evinces strong congressional recognition of the difficulty of getting people with alcohol and drug problems into treatment.

The conferees wish to stress their conviction that the strictest adherence to...[confidentiality] is absolutely essential to the success of all drug abuse prevention programs. Every patient and former patient must be assured that his right to privacy will be protected. Without that assurance, fear of public disclosure of drug abuse or of records that will attach for life will discourage thousands from seeking the treatment they must have if this tragic national problem is to be overcome.²

The problems of alcohol and drug abuse reach into all classes and all races, and unfortunately continues to be very stigmatizing for all who suffer from them, even after years of successful recovery. A wrongful disclosure of

² H.R. Rep. No. 92-920, 92d Cong., 2d Sess., p. 33 [in U.S. Code Cong. & Admin. News, 1972, p. 2072].

patient identity can end a career, destroy a marriage or devastate a friendship. The attitudes of employers, family and others even toward substance abusers in recovery remain plagued by misconceptions and discrimination. The consequences of the labels "addict" and "alcoholic" are painfully obvious to anyone in treatment, out of treatment, or, perhaps most importantly, contemplating treatment.

Treatment programs enroll and treat some of the most difficult populations to reach and serve: pregnant and parenting women; persons infected with HIV; young people at risk for involvement with the criminal justice system. Many of these individuals have traditionally been suspicious of government programs, medical services and other institutions. It is often because substance abuse programs have carved out identities distinct from some of these systems that many people can be encouraged to come into and remain in treatment.

To avoid or minimize the stigma associated with alcohol and drug abuse, the federal statute and regulations established strict confidentiality provisions. Thus, a specialized alcohol and drug program may make no disclosures which reveal that an individual person is receiving diagnosis, referral or treatment except in a few specifically delineated circumstances such as a medical emergency or in instances of suspected child abuse. This principle is a fundamental tenet of such programs. Staff and clients are trained that the fact that people have sought and or are receiving treatment or other services is

simply not public knowledge, even to people who might generally have the authority or family relation to obtain medical information about an individual. The personal and volatile nature of this information requires that it be carefully protected for treatment to succeed.

Of course, the federal alcohol and drug confidentiality law does allow disclosures in situations where communication of information is desirable or necessary. In our experience, every reasonable request for disclosure of patient information can fit one of the conditions provided by the statute.

The most common way for alcohol and drug programs to disclose information is via written consent of the patient. The consent process encourages narrow specific requests for information. Disclosures can be made with patient consent to insurers, employers, members of a client's family and anyone else. A key feature is that the recipient of information provided pursuant to a consent may not redisclose that information without proper consent or other authorization. The consent process is often used by the provider as a way of educating the client to particular issues which may come up during treatment. For instance, if programs routinely ask clients for TB tests, a discussion when they sign a release for the reporting of this information to public health provides an opportunity to educate the client about the risks and prevention of TB.

In our experience, clients come into and stay in treatment because of privacy protections afforded by the law and regulations. Our clients are

persons whose very addiction involves socially marginal and often illegal activity. These people are extremely vulnerable — especially at the point of entry into treatment — and need privacy to make the transition to recovery.

**The Existing Federal Law Is More Effective Than The Act
Subpoenas**

The federal confidentiality laws for alcohol and drug patient records are superior to the proposed Act in a number of important respects. Every day, specialized alcohol and drug treatment programs receive subpoenas for their patients treatment records for use in proceedings where these records are not relevant, the information can be obtained elsewhere, or the request is made to obtain information solely to impugn the character of someone in a court proceeding by labeling him a drug user. Under the existing federal laws, a specialized alcohol and drug program may not comply with such a subpoena (1) unless the patient has consented or (2) there has been a court proceeding in which a judge has made a determination that "good cause" for ordering the disclosure exists because the need for the treatment records outweighs the client's privacy rights in the information. 42 C.F.R. § 2.61 - 67.

The regulations thus steer sensible middle course to protect against willy — nilly disclosure of highly personal information, but allowing such orders to be issued when appropriate. The court—order provision requires that an entity

requesting such an order give notice and opportunity to be heard to the program and client and allows for the court's in camera inspection of patient records.

When DHHS published its commentary to the Final Rule (52 Federal Register at 21801—2, June 9, 1987) it included comments about the importance of the safeguards in the court order provision which are instructive:

Most comments in opposition to relaxing the court order limitations on confidential communications said that the potential for disclosure of confidential communications will compromise the therapeutic environment, may deter some alcohol and drug abusers from entering treatment, and will yield information which may be readily misinterpreted or abused...

A typical subpoena which arrives at alcohol and drug programs is issued by an attorney for an estranged spouse in divorce or child custody proceedings. The request often reads "For all the treatment records of Mary Doe". It is often the case that the attorney has other ways of obtaining information about Mary Doe, but the treatment program is an easy target. More important these subpoenas often seek all kinds of personal information about the client which has little or no relevance to the proceeding at hand, but which can become wildly prejudicial and damaging.

Unlike the regulations, the Act does not require that subpoenas be accompanied by court orders. The presumption in the Act is that a request by subpoena, whether or not from law enforcement authorities, is sufficient for the health information trustee to disclose information. The burden for bringing a motion to quash is on the individual who may not have actual notice of the subpoena.

Law Enforcement

Another important check on the disclosure of alcohol and drug information provided by 42 CFR 2 but lost in the Act is in the area of investigations of suspected or actual criminal activity. Because addiction involves the use of illegal drugs, persons seeking treatment for addiction are very vulnerable when they first enter treatment and in later stages due to their past criminal activity. Congress recognized that control of drug abuse and its collateral criminal consequences would be thwarted if individuals who had been addicts were subject to unchecked disclosures from their records or by their counselors because fear of arrest would deter most from coming forward for treatment at all.

Thus, under the federal alcohol and drug confidentiality rules, an investigative, law enforcement, or prosecutorial agency must obtain a court order to obtain information from an alcohol and drug program, even if the law

enforcement officials have a search warrant. Before a court order can be issued an order to disclose information for purposes of investigating or prosecuting a patient for a crime, the a court must find that: (1) the crime involved is extremely serious; (2) the records sought are likely to contain information of significance to the investigation or prosecution; (3) there is not other practical way to obtain the information. 42 C.F.R. § 2.65. Note that the kinds of "serious crimes" for which a court may order disclosure of patient records does not include possession or sale of illegal drugs. Allowing orders to be issued to investigate drug offenses would allow disclosure of treatment information about all illegal drug users, which in turn would lead to the nightmare scenario so worrisome to Congress that no one would enter treatment for fear they would be arrested.

This issue remains probably the most important to alcohol and drug programs, yet the Act does not provide any of these important protections. The Act simply allows law enforcement officials to execute any warrant on subpoena without notice or careful judicial screening. As a result, alcohol and drug programs would have to disclose identities of clients, not only if they were the subject of an investigation or prosecution, but also if they were a witness or a figure in a mere inquiry conducted by law enforcement. Such a program could also have to comply with a grand jury subpoena. These requirements do not protect the clients who for instance are in treatment at great risk from their former associates who are still using or dealing drugs.

Under the Act, an attorney representing an accused drug dealer, for instance, could easily obtain information about a newly admitted client, who was a witness to a drug deal, by subpoena. The client and the program would lose the protection to avoid or limit such disclosures currently provided under the court order provision in the regulations.

The purpose of the protections of 42 CFR 2 are not to thwart important criminal proceedings. The existing federal laws permit disclosure of all necessary information for the investigation or prosecution of serious crimes by alcohol and drug programs — but Congress recognized that unless key protections were in place, the goals of treating addicts would be seriously undermined.

Disclosures to Family and Next of Kin

It is difficult to imagine an area of more sensitive disclosures or one in which the patient is more vulnerable to pressure than in the area of disclosures to family members. The federal alcohol and drug confidentiality law provides crucial protections for clients dealing with families because alcohol and drug abuse can be intricately involved in family dynamics. For instance, an alcoholic may be fearful to tell family members, who also drink, that their drinking is out of control and they have decided to seek help. So, unless a

client consents to the disclosure of any information about their treatment to a family member, such information is not available to them.

These protections have been especially important for women entering alcohol and drug treatment. For instance, women are often in relationships with men who encourage their use of drugs or alcohol and disapprove — sometimes violently — of a woman's seeking treatment. Also, women are often using drugs and alcohol to numb the pain of sexual abuse from lovers or family members. Thus, alcohol and drug programs understand that clients will often not want certain family members to even know that they are in treatment and that it may not be therapeutic for them to know. This is also common in couples where both partners abuse alcohol and only one seeks treatment.

The written consent process in the regulations has been useful in preventing unwanted disclosures to family members. Clients know that without their written consent, family members will not be told about their treatment. This reassurance is lost under the Act. For instance, Sec. 124 allows a health information trustee to disclose protected information to the client's next of kin without specific consent of the individual. The section does prohibit the disclosure if the individual has previously objected to the disclosure, but this is far less protective than the affirmative standard provided by a requirement of written informed consent. Under this section, a provider may disclose treatment information to a partner of a client who did not previously object to the disclosure. In an area where family relationships are often shifting and can

be devastated by an untimely disclosure of treatment information, this is a major loss of privacy for the individual in alcohol and drug treatment.

Disclosures to Employees

Another area in which alcohol and other drug clients are extremely vulnerable is in their relationship with their employers. Under the federal alcohol and drug confidentiality law, other than by consent, information identifying an employee as being in treatment would virtually never be given to an employer. Many clients are in treatment which is paid for wholly or partially by employers. If this is the case, they may consent for information necessary to payment to be disclosed to an employer. Usually however, the employee fills out a claim form with an insurer and only limited information goes back to the employer, via consent.

Under the Act, health information trustees and payers exchange information without specific consent of the client. In the case where treatment is paid for directly by employers, there is not any provision comparable to the consent form for the narrowing of information which is ultimately provided to the employer. Without the protection of a narrow consent requirement, employers are potentially recipients of very personal treatment information.

Because of the stigma attached to alcohol drug dependence, many persons with this illness are very vulnerable to termination by their employers, even if they have had no work performance problems and enter treatment voluntarily. As a result, they often keep both their substance abuse and treatment hidden from the employer. This may especially be true if the treatment does not require absence from work and is not paid for by the employer. In such a case, the employer would almost never receive patient identifying information from a program under the existing federal regulations.

However, the Act lacks the level of protection necessary to prevent very damaging disclosures to the employer. For instance, the Act permits patient identifying information to be listed on a directory and to be provided "to any person". Sec. 124(b). Directory information can include the name of the person, their general status and that they are in a program. The recipient of this information is not bound by law to not redisclose that information. So, a co—worker of a patient whom they believe to have a drug problem could call up a treatment program, confirm that the co-worker is in treatment and in turn tell the employer this information.

Surely we would hope that an employer would not make an adverse employment decision against the client solely because he/she is in treatment. Unfortunately, however they sometimes do, though they may not admit that it is the actual basis for dismissal. If an employer did decide that the patient should be fired for "being a drug user", the Americans with Disabilities Act of

1990 (ADA) unfortunately would not protect the patient if he or she is a "current user of illegal drugs". The ADA provides no protection even if the individual recognized the problem and entered treatment, and was performing his or her job satisfactorily. Thus, disclosures to employers which are permissible under the Act could have devastating effects on the employment of alcohol and drug dependent persons, and even those in recovery.

HIV/AIDS Information Confidentiality

LAC is also very concerned in our practice about the confidentiality of information concerning people with HIV and AIDs. A great number of the clients of alcohol and drug programs are at high risk for or have these infections. As a result, we have seen how crucial the confidentiality of their status is both in dealing with their addictions and in the community at large.

We have worked closely on the development of New York State's HIV/AIDS confidentiality laws and have also examined similar statutes in many other states. It is our belief that the Act should not preempt state laws which provide more privacy protection for this kind of information than it does.

For instance, many state laws on testing for HIV narrowly limit the people who may be told of a patient's HIV positive result. In our experience, this kind of information, just like alcohol and drug information, is extremely

volatile and can have positive or devastating effects on someone's treatment depending on how the information is handled.

For instance, when the disclosure of HIV test information is handled through a written consent, such as required under New York State Public Health Law, Sec. 278 *et seq.*, the medical provider can use the process to counsel and educate the patient about how to best manage his medical treatment, who else is at risk if he tests positive, and what kinds of behaviors had needs to change. At the same time, the client can assert his needs for privacy from people whom he believes will not act in his own best interest.

The Act does not require written consent for such a disclosure, and in some sections, would allow for the disclosure of this information to next of kin. For instance, Section 155(b) of the Act states that if a health care provider determines that a patient cannot "knowingly or effectively" act in his or her own interests, the next of kin may exercise the patient's rights to authorize disclosures. Of course, exercising the right to authorize disclosures of HIV related information implies that the health care provider will give such information to the relative. However, there is no judicial determination of whether the patient is or is not competent, rather this is left to the determination of the health care provider. Neither is there a prohibition on disclosure to a relative whom the client previously objected to receiving that information.

In our experience, many HIV positive persons have decided not to give that information, for instance to their parents or other persons in their family. A disclosure of HIV—related information necessarily implies information about the most private of human behaviors. Many state HIV confidentiality laws are more protective about who and how is given this information than the Act. This kind of disclosure can easily do more harm than good.

Legal Action Center supports the concerns about preemption of State HIV confidentiality laws expressed by organizations such as AIDS Action Council in their written and oral testimony.

Conclusion

Legal Action Center appreciates the importance this subcommittee is placing on the need for federal privacy legislation in health care reform. As detailed here, we believe that existing federal legislation already adequately protects the records of persons in specialized alcohol and drug programs, and does so much more effectively than would the proposed Fair Information Privacy Act. Our experience serving such programs and their clients is that confidentiality protections in 42 U.C.S. 290dd, ee-3 are uniquely tailored for their needs. To continue the national efforts at controlling alcohol and drug dependence, we believe this statute and implementing regulations must remain

in effect and not be pre-empted by whatever confidentiality provisions Congress enacts as part of national health care reform.

Thank you for your attention.

Mr. CONDIT. Thank you, Ms. Jacobs. Ms. Goldman.

STATEMENT OF JANLORI GOLDMAN, DIRECTOR, PRIVACY AND TECHNOLOGY PROJECT, AMERICAN CIVIL LIBERTIES UNION

Ms. GOLDMAN. Thank you. I want to thank you, Mr. Chairman, and the members of the subcommittee for holding these series of hearings on privacy in health information and also to applaud you for your commitment to enacting comprehensive Federal legislation in this area. This subcommittee has truly taken the lead in Congress in looking at this comprehensive privacy legislation.

The bill that you have introduced, Mr. Chairman, H.R. 4077, represents a substantial consensus among very diverse groups. As you have heard yesterday and a couple of weeks ago, there is substantial agreement on this bill. This is an incredible achievement, given who you have had testify.

We do still have a way to go. There are still some issues to resolve. I want to say at the outset that, regardless of the issues that we need to resolve, I do not want us to lose sight that H.R. 4077 holds the promise of doing today or maybe tomorrow what the Administration says will take 3 years to propose.

In the administration's bill, as you know, there is a provision which would have a national health board proposing Federal legislation on privacy 3 years after the date of enactment and then Congress would still have to act on it.

I think that this subcommittee has shown that it is possible—with a great deal of effort and time, to put together a privacy bill which is comprehensive and which has the support of diverse groups.

The thing which I think is remarkable about the bill is that it would offer uniformity across the States while still providing the strongest protection at the Federal level, stronger than anything we currently have at the State level.

The bill would allow disclosures for payment and treatment purposes and with fairly rigorous standards, allow disclosure for public health purposes. For all other disclosures, you would have to get the individual's consent. Individuals would have a right of access to information about them and, as you have heard, the enforcement provisions of the bill are very strong and very necessary.

We have a few recommendations for strengthening the bill, for expanding the scope of the bill, which I will try to go through fairly quickly.

As we have heard, preemption is a major issue of concern, not only for the ACLU but also for other groups that have testified. What we would like to see—and I know that we are all working toward this goal—is that we not stop the flow of information State by State. We should encourage the flow of information, but we should still allow the States some leeway in enacting legislation to go above the Federal standards.

Again, I want to stress that this is a hypothetical situation since, currently, H.R. 4077 would provide a higher level of protection than what States currently provide. In the event that either the Federal law is weakened or the States feel that they have a need to enact stronger legislation in a particular area, I think that we should try to provide some leeway for them to do so.

Second, on the section on protected health information, there have been a number of people who have raised a concern about trying to expand the scope of protected coverage for protected health information. Currently, the information which is protected is that which is created and maintained for treatment and payment purposes. There has been some concern, which we share, that there are other kinds of health information generated in other contexts, which we should also try to protect. The employment context is possibly the largest area not covered by the bill, including for instance information generated in preemployment screening.

We do recognize, however, that we cannot protect every piece of health information in the universe and that this bill still does protect a substantial amount of information.

The other area that we would like to see improved on is the next of kin and directory information section—section 124. A straightforward way of improving that section would be to provide individuals with notice of the right to object to disclosure. It is a simple provision and would take care of the concerns that we have heard raised in the last couple of days.

If people know that they have the right to object, they will then be able to, in a more meaningful way, decide whether or not they want to withhold information from their next of kin.

The other concern we have about that provision is that it would allow for disclosures pursuant to or consistent with accepted medical practice. I am not really sure what that means. I am not sure that people reading the bill would know what it means, either. I would just suggest that we leave that provision out and set the standards more clearly.

We have two concerns about health researchers, as defined in the bill. They are currently defined as “public health trustees” and we think that that is too broad a category for them.

We would like to see the provision for health researchers moved into “special purpose trustees” so that health researchers receiving information for one limited purpose may use such information only for that purpose, whereas public health trustees have a much broader mandate.

On alternative dispute resolution, we also agree with our colleague from the AIDS Action Council that ADR should not be mandatory and that it should not preclude an individual’s ability to come into court, although we appreciate that it is being encouraged and it may be a worthwhile way to try to resolve disputes outside of court.

Our last suggestion deals with the disclosure provision in H.R. 4077. Disclosures under the bill are allowed within institutions. Disclosures are defined as any disclosure made within an institution.

Our position is that not everyone within an institution should be able to look at an individual’s health information. For instance, there may be a particular doctor who has absolutely no need to look at the information. You might have an administrative person or a janitor, who also has absolutely no need to look at the information.

What we would recommend is that, under the use section of the bill, section 121, where there is a very clear standard that is set

forth for using information, which is that it has to be compatible with and related to the purpose for which it was collected, we would suggest collapsing the disclosure and use provisions so that, even within an institution, information could not be disclosed unless it was compatible with the purpose for which it was collected. I think that would still allow for broad latitude in terms of disclosure and use.

I want to just close by saying again that the work of this subcommittee and of the staff has been really tremendous in achieving a significant consensus on this bill. We have a very good opportunity to pass this legislation this year. I appreciate all of the work that has been done.

[The prepared statement of Ms. Goldman follows:]

Testimony of Janlori Goldman

Director

ACLU Privacy and Technology Project

Before the

Government Operations

Subcommittee on Information, Justice,

Transportation and Agriculture

Regarding H.R. 4077:

The Fair Health Information Practices Act of 1994

May 5, 1994

Chairman Condit and Members of the Subcommittee:

I very much appreciate the opportunity to testify before you today on behalf of the American Civil Liberties Union's (ACLU) Privacy and Technology Project. The ACLU is a private, non-profit organization of over 275,000 members, dedicated to the preservation of the Bill of Rights. The Privacy and Technology Project was established in 1984 to evaluate the impact of new technologies on individual privacy.

I. OVERVIEW

The Project's primary goal for the 103rd Congress is the passage of federal legislation that establishes enforceable privacy protection for personal health information. The need for such legislation is the most critical privacy issue facing this country today. As our nation continues to debate the reform of the health care system, protecting the privacy of peoples' health records must be at the heart of any health reform effort. In fact, legislation to protect people's health information is needed even in the absence of comprehensive health care reform.

Health care reform cannot move forward without assuring the American public that the highly sensitive personal information contained in their health care records will be protected from misuse and abuse. If people are expected to embrace a reformed health care system, the price of their participation must not be

a loss of control over the sensitive information contained in their health care records.

H.R. 4077, the "Fair Health Information Practices Act of 1994," is a necessary and long-awaited response to the absence of a comprehensive federal law to protect peoples' health records. This bill is the most important piece of privacy legislation pending today, and we applaud its introduction. H.R. 4077 is the culmination of many months of work by a diverse coalition of industry representatives, consumer advocates, representatives of the AIDS community, the ACLU, and health policy specialists. While delivering near uniformity of standards and process to the health care industry, the bill more importantly guarantees to Americans that their personal health information will be vigorously protected against unauthorized and unnecessary disclosures. As of today, the bill represents a substantial consensus among the affected groups. But we still have some work to do. The promise of H.R. 4077 is accomplishing today what the Administration proposes will take three years.

We applaud you, Mr. Chairman, for taking the lead on this issue -- both through the introduction of H.R. 4077, and the series of hearings you are holding on health record privacy. Our statement outlines the pressing need for federal legislation that creates an enforceable privacy right for personal health records and our recommendations for strengthening H.R. 4077.

II. H.R. 4077 AND THE ADMINISTRATION'S HEALTH SECURITY ACT

We believe H.R. 4077 is consistent with the principle set forth in the privacy section of the President's Health Security Act. According to the testimony of Nan Hunter, Deputy General Counsel of the U.S. Department of Health and Human Services (HHS) before this subcommittee on April 20, 1994, the Administration welcomes H.R. 4077 and is willing to work with Congress towards the passage of comprehensive federal legislation to protect medical records. HHS stated that the Administration is "pleased that [the sponsors of H.R. 4077] share [HHS's] vision for careful, respectful treatment of health information."

From a privacy standpoint, the President's health reform proposal is inadequate. The Administration envisions a system in which all of the responsibility for developing privacy standards and legislation is delegated to a National Health Board. From the date of enactment, the Board is given two years to promulgate standards for the privacy and security of individually identifiable health information (§ 5120(a)), and three years to submit a legislative proposal to provide a comprehensive scheme of federal privacy protection (§ 5122). The Act requires that, in developing legislation and standards, the Board must incorporate principles of fair information practices.

H.R. 4077 is the realization of the Health Security Act's

vision, three years ahead of schedule. In its April 20th testimony, HHS acknowledged: "[H.R. 4077] offers immediate federal protections for all health care records. We welcome this proposal, and are eager to work closely with you on it."

H.R. 4077 provides a comprehensive scheme for federal privacy legislation that embodies the principles and goals of the Administration. Under H.R. 4077, individuals may obtain their own information (§ 111) and consent to disclosures to third parties (§ 122). Law enforcement is given limited access (§§ 129, 123). Further, there is a general bar on unauthorized uses (§ 121) that prohibits disclosure to employers. Finally, individuals will be given notice of how information will be obtained and used (§ 114).

H.R. 4077 is a powerful and workable response to the public clamor for federal privacy protection of health care information.

First, and perhaps most importantly, H.R. 4077 establishes principles to be followed in most circumstances in which personally identifiable health care information is used. Any use of personally identifiable health care information must be compatible with and related to the purpose for which the information was collected or maintained. Any disclosure of the information must be limited to the minimum amount necessary to accomplish the purpose of the disclosure.

Further, individuals about whom medical information is collected and maintained have a right under this bill to see and correct any such information maintained by health care organizations. They must be notified concerning any disclosures made of their information. Other than disclosures for treatment, payment or legally authorized public health purposes, disclosures of personal health information may be made only upon consent of the individual about whom the information is maintained. In addition, there are a small number of non-consensual disclosures that may be made. The bill details such disclosures and provides specific guidelines to be followed when such non-consensual disclosures take place, such as for emergency circumstances and law enforcement.

More specifically, H.R. 4077 furthers the important dual purpose of allowing certain patient-specific information to flow among various entities. For example, it is important that health care providers have access to relevant information possible concerning the medical condition of an individual. This bill allows disclosure of this information in the treatment context. Also, public health authorities need to track various diseases in an attempt to eliminate and control them. This bill allows these disclosures as well. Finally, insurance companies and other third-party payors need certain information before they can process an insurance claim and pay a provider. Again, H.R. 4077 permits this relay of information.

III. RECOMMENDATIONS

While we hail the introduction of H.R. 4077 and look forward to its passage, we recommend the following changes to strengthen the bill:

1) The preemption of state laws by H.R. 4077 is an important provision of the bill. The intention of the interests supporting the legislation is to achieve uniformity while providing the strongest possible protection for personal health information. We are continuing to work together to create language that reflects this goal;

2) H.R. 4077 limits the scope of privacy protection coverage. Only personally-identifiable health information that is "created or maintained as part of the health treatment and payment process" is protected¹. Indeed, the definition of "protected health information" includes only information that "relates to . . . the provision of health care to an individual, or payment for the provision of health care to an individual."² We believe it is essential that federal confidentiality legislation protect as much personal health information as possible.

¹ See §2(b)(1).

² §3(a)(3)(B).

- * We suggest that the definition be broadened to include all information, no matter how created or obtained.

A practical example in which the protections in H.R. 4077 fall short of full coverage is in pre-employment screening. Often a physician will ask an individual basic questions concerning his or her personal health history. None of this information would be protected by H.R. 4077 because it was not obtained in the course of the provision of or payment for health care. This gap can be filled by broadening the definition of "protected health information" to include all health information, no matter its origin;

3) Another provision we believe should be strengthened is the next-of-kin and directory information section (§ 124). This section provides individuals about whom medical information is compiled to object to disclosure to "a person with whom the individual has a personal relationship." This language does not go far enough because it fails to require the necessary component of notification to the individual of his or her right to object. Without notice a waiver of this right will not be meaningful;

- * §124(a)(1) should be amended to allow disclosure to next-of-kin if "the individual **has been notified of the right to object** and has not previously objected to the disclosure."

4) Another area of the bill we find troublesome involves health research. A health researcher falls into the category of

"public health trustee" for purposes of this bill. (§3(b)(8)). While we strongly support restrictions on health researchers' abilities to disclose information, we do not think the "public health trustee" category contains the appropriate limitations on these powers.

Section 125, regarding public health, states that public health trustees may obtain information "for use in legally authorized disease or injury reporting, public health surveillance, or public health investigation." Public health authorities should receive such information. Health researchers should not, unless, of course, such information is necessary to an IRB-approved research project under their supervision. It is simply not appropriate that a health researcher be authorized by federal law to use information so broadly.

- * Health researchers should be moved from the "public health trustee" category to the "special purpose trustee" category.

Further, the health research section itself (§128) needs to be strengthened. This section states that information may be disclosed to a "public health trustee" so long as certain requirements are met. Our concerns regarding this section are two-fold. First, as outlined above, we feel that a health researcher be considered a "special purpose trustee" for purposes of the bill, or even simply as a separate category of "health researcher."

Second, one requirement for disclosure under this section is that an IRB must determine that the research project would be "reasonably impractical to conduct without such information." We fear that this language is too vague and broad;

- * An actual, clear standard is necessary for this apparent restriction to be effective.

5) We urge that the section dealing with alternative dispute resolutions (§163) be clarified. While the use of alternative methods for resolving disputes certainly should be an option for aggrieved individuals, it should not be a mandatory method. That is, ADR should be one of a few options for resolutions of claims under H.R. 4077.

The Health Security Act outlines specific procedures for ADR that may be helpful here. Under the Administration's proposal, the individual decides **whether or not** to utilize alternative dispute resolution methods. If the individual so decides, the other party--in our case, the health information trustee--must participate (§5212). Further, the findings and conclusions of the mediator are "advisory and non-binding." (§5214(a)). This section goes on to say that "[e]xcept as provided in subsection (b), the rights of the parties under subpart A shall not be affected by participation in the program." That is, other options for resolution, including litigation, are not foreclosed. If, however, the parties agree to settle, the signed settlement agreement is binding (§5214(b)), and courts will enforce these

agreements (\$5215).

- * It is important that the alternative dispute resolution methods be an option for individuals' to enforce their rights under H.R. 4077; however, such resolution techniques should not be mandatory. Incorporation of the provisions of the Health Security Act would be helpful in this effort to clarify and strengthen the ADR section of the Condit bill.

In addition to the recommendations above, there are a few minor, more technical changes we believe are necessary.

1) In need of clarification is the definition of "disclose" in section 3 of H.R. 4077. Under this definition, communication of personally identifiable health information within a health care institution--i.e., to an "officer or employee" of a health information trustee--is not a disclosure. As the language stands, **any** employee within a health care institution may receive information about an individual for **any** reason, from the chief of staff through the janitor. While it is important to allow transmission of information within a medical facility, both for treatment and payment, it is unnecessary for all information to be made available to all employees.

- * If this definition of "disclose" remains, insert a standard to govern transmission of sensitive health information to employees of the HIT. It is probably best to incorporate the standard for "use" of health information found in §121--i.e., the information may be used only for a purpose "compatible with and related to the purpose for which the information was collected or was received by the trustee."

2) Section 102, which delineates the duties and authorities of public health trustees, should be clarified. Subsection (3)(A) states that a public health authority may disclose information if "such disclosure is essential to fulfill a public health purpose." There is no guidance here concerning the scope of the vague term "essential." Further, disclosures for public health purposes are allowed by §102(3)(B)(ii), if made in accordance with the limitations set forth in sections 121 and 125. We agree that there must be strict standards governing the disclosure of information for public health purposes; however, the current language does not achieve this desired result. At best, §102(3)(A) is redundant in light of §102(3)(B)(ii); at worst, it is confusing both to the present reader and potentially to future courts attempting to interpret H.R. 4077.

- * Section 102(3)(A) should be deleted from the bill, and disclosures for public health purposes should be allowed in accordance with §§ 102(3)(B)(ii), 121, and 125.

3) A final provision of H.R. 4077 that needs alteration is §126, concerning emergency circumstances. Under the current language, there is little guidance for the determination of what constitutes an "emergency circumstance." By shoring up the standard in this section, it will become easier for health information trustees to know their rights and obligations in these circumstances.

- * The following is proposed amended language:

A health information trustee who

is authorized by subtitle A to disclose protected health information under this section may disclose such information in emergency circumstances when necessary and appropriate to protect the health or safety of an individual.

CONCLUSION

H.R. 4077 is the culmination of a tremendous effort by a diverse group to achieve substantial consensus on health information privacy. We commend your leadership on this critical legislation. Congress has both the opportunity and the responsibility to seize the chance created by the current focus on health care reform and to enact H.R. 4077 with our recommendations.

Mr. CONDIT. Thank you very much. We have a series of questions to ask all of you. If you agree with each other, you can just say, "I agree with that," and we can shorten it up a little bit.

How would you assess the general level of protection for health information under this bill, H.R. 4077, as compared with existing law? Ms. Berenson, we will start with you and just go down the line.

Ms. BERENSON. I think that the level of protection in H.R. 4077 is better than what we currently have in some States and not as good as what we currently have in other States with regard to HIV confidentiality laws.

I think that is where our concern comes in. We would want to see the protections here be a floor, because there are some States—and I discussed them in my written testimony—that have really worked very hard to develop more protective State HIV confidentiality laws, particularly in response to crises within the State.

I think that it is an appropriate thing for Congress to create a floor and leave to the States the ability to respond appropriately to instances where they believe the health, welfare, and safety and protection of their citizens requires some greater protection.

Mr. CONDIT. Ms. Jacobs.

Ms. JACOBS. I would agree with Ms. Berenson. I just wanted to clarify that the alcohol and drug patient records are not controlled by State law. In fact, 42 U.S.C. has preempted any State law on that, so it controls the field.

Ms. GOLDMAN. In the research that we did looking at the State laws, generally what we found is that the provisions in 4077 are stronger than what you find at the State level. There may, as my colleague said, be some exceptions but overall, H.R. 4077 would be the strongest and most uniform Federal law that we could possibly have, given our need, also, to achieve consensus among the affected groups.

In terms of the Federal law that deals with drug and alcohol treatment, it is important that that law stay in place and that 4077 not supersede it that or not preempt that. Generally, the ACLU is opposed to preemption of State law in the area of privacy and consumer legislation. We are fighting preemption right now on Fair Credit Reporting Act legislation. We have fought it in other areas.

What we see is that what we are able to achieve at the Federal level is usually not nearly as strong as what the States are able to enact. There are many States—California, for instance—where they are extremely progressive in the areas of privacy and consumer law and we do not want the Federal law to undermine those efforts.

This bill provides an exception to our general rule against preemption in privacy statutes for us in that, thus far, it is the strongest and most uniform legislation in this area. My only concern, as I stated earlier, is that this bill may be weakened over time.

Congress may, at some point, do something which would undermine some of the strong provisions currently in it, and we should leave some provision in the preemption section that allows for the States to enact stronger legislation that would impede the electronic dissemination of information.

Mr. CONDIT. Some of you were here yesterday and you heard the discussion. There seemed to be a strong recommendation for preemption, uniform preemption. You, Ms. Goldman, do not think that we ought to do preemption at all.

Did anyone else hear the testimony—I know you did—yesterday? Do you have any thoughts about their suggestions? How far should we go with preemption? I know Ms. Goldman's view on it. How about the two of you? Do you have any specific recommendations on preemption?

Ms. BERENSON. I As I stated earlier, I think that the Federal law should preempt any State laws that do not provide greater or equal protections.

Part of the difference in how we view preemption and how certain institutions may view preemption is that when we are thinking about the State laws that we would not like to see preempted, we are thinking about substance. We are thinking about laws that provide greater substantive protection.

I think, to the extent that there is a concern that allowing greater substantive protection would impede the ability to have uniform processes or procedures for transmitting and collecting and maintaining information, I think that is something that can be worked out. I do not think that the two are necessarily in conflict.

Mr. CONDIT. Let me just ask, then—because I think there is general agreement among the three of you—does anyone here disagree with Federal preemption for technical and administrative standards for electronic data interchange?

Ms. JACOBS. No.

Ms. BERENSON. No.

Ms. GOLDMAN. No.

Mr. CONDIT. OK. One of our colleagues has to leave. I want to give her the opportunity to speak or ask questions. Ms. Woolsey.

Ms. WOOLSEY. Thank you very much, Mr. Chairman. I am sorry. I, too, have to go to testify before the Appropriations Committee.

Because I am from California, I definitely want States to have the option to enact privacy legislation that is stronger than the Federal Government's. I was a human resources professional for 25 years so there are two areas that I would like to talk about. One is employee assistance programs and the other is preemployment screening.

My clients in the company where I was the human resources director always knew that we did not take action unless it was based on job performance. Certainly, we did not fire somebody because they were an alcohol or a drug addict but, if their performance was affected, we would send them to employee assistance and treatment programs.

Now, my question is, where in your proposals can the employer be privy to the information about whether their employees are attending the programs and that it is working?

Ms. GOLDMAN. What we would like to see is, as Congressman Sawyer talked about earlier, a functional separation within a company between employee assistance programs and other company records. The information that is generated in the course of providing treatment and providing assistance must be kept absolutely separate—

Ms. WOOLSEY. Locked.

Ms. GOLDMAN[continuing]. Locked, separate, firewalls—whatever legal and technical mechanism can be created to ensure that information is not made available outside of the treatment context.

Ms. WOOLSEY. Do you agree, Ms. Jacobs?

Ms. JACOBS. Basically, and I would just add that, as you probably know, some EAPs are now protected under 42 U.S.C. 290 if they are federally assisted and meet the whole other standard. To the extent that ones are not, then I would agree with what Ms. Goldman is saying about how those records should be kept.

Ms. WOOLSEY. That is exactly what we did with my client companies and also with preemployment screening. The screening was based on job-related issues only and we had the information in a separate file, locked, only available to the people that it was pertinent to—the personnel person and the hiring manager or supervisor.

Should we have done more? Are you recommending more?

Ms. GOLDMAN. The ACLU is recommending more in 4077. Unfortunately, that information is not covered by the bill and I think that it should be. I think we should find some way to draft language to expand the scope of the bill so that it is not just treatment and payment but also information that is generated in the process of a preemployment screening.

Ms. JACOBS. One could look at the language, again, of 42 U.S.C., because it is instructive in terms of what is a medical record and talks about information both for treatment and for initial referral and diagnosis and, when a preemployment discussion turns into, “By the way, do you have any conditions I ought to know about or do you want to tell me anything else,” and suddenly there is a whole disclosure, that might wind up being protected information.

Ms. WOOLSEY. If interviewers are trained correctly they will ask about any information that relates to the job that they are interviewing for.

When we do things like this, we come in all heady and intellectual about the issue at hand. But then, I was sitting here listening to you and all I could remember was, in 1980, having blood transfusions and, in the middle of the 1980’s, getting a letter saying, “Go get HIV tested,” because that was before they screened blood for the HIV virus.

At that time I was a person in my community that was well-known, and so, I went through the whole question of, “Do I sneak into the clinic; what do I do?” I made the decision to walk in, just go through the process, go to the local lab, have the test and, if anything came of it, then wouldn’t I be a good example of the fact that all kinds of people could be in trouble? I think I knew that I was healthy and that it would be fine.

I agree with you, we have to be very careful about what we do with people’s health records. One of our colleagues talked to us 2 weeks ago about what had happened to her when her medical records were made public and how damaging that could have been to her entire life. Please keep us informed about how to ensure privacy of medical records and how to do it without people thinking they are protected if they are not.

I particularly want you to tell us about how we should educate the public about what their rights are with regard to this issue. If anybody wants to comment on that, go ahead.

Ms. BERENSON. As I stated in my written testimony, the very situation you are talking about is part of the problem.

I think that particularly for people who, unlike yourself, do believe that they are at high risk for being HIV-positive, the fear of what will happen if they go to get tested or go to get treated and that information is released without their consent is very real—we know people lose their jobs, they lose their homes, they lose their friends and families. These things may be illegal, but it is sort of late in the game to discover that you have the right to sue under the ADA.

What we want to try to do is create a situation where we really feel comfortable that we have strong, uniform protections, that we can educate people about what those protections are and empower them to make decisions with knowledge that will, overall, be in their best interests and in the public's best interests.

Ms. WOOLSEY. Then one of the things I would recommend—and, to you, Mr. Chairman, also—is that the forms that everyone must sign concerning the confidentiality of medical records are simple. Nobody reads that stuff, when they go into a doctor's office or a lab and they are handed pages of little, tiny print. People just sign it.

So, let's make the forms straightforward and easy to read so people know what they are signing. Thank you, Mr. Chairman.

Mr. CONDIT. Mr. Horn.

Mr. HORN. Thank you very much, Mr. Chairman.

You mentioned, I believe, Ms. Goldman, that you had some examples of where the State laws would be much stronger. I wonder if you could furnish them for the record.

Mr. Chairman, before you leave, on the issue of State laws and could they be stronger than what is in this bill, I wonder if perhaps you could not request the American Law Division of the Library of Congress to search State laws and furnish for the committee, and we put it in as an exhibit, where are the States on some of these issues, such as either informed consent or notifying the next of kin? Could we just sort of find out, because I think it would be better if we knew before completing the hearings?

Mr. CONDIT. We have the information available to us.

Mr. HORN. Is this done by an objective source such as the Library of Congress or is this all advocacy selection?

Mr. CONDIT. I don't know who the sources exactly are but we can provide you with that and then, if it is not—

Mr. HORN. I would like to hear what examples you had but I would also like to make sure the American Law Division—

Mr. CONDIT. Let me do this, Mr. Horn. I can provide you with the information we have.

Mr. HORN. OK.

Mr. CONDIT. We are going to revisit this issue again. If you are not pleased with the information we give you, then we can sit down and discuss it.

Mr. HORN. I have no way to know if I am pleased or displeased because I am not searching the records. I just think we ought to know ahead of time, what are we fixing.

Ms. JACOBS. Mr. Chairman, I can give you a quick answer.

Mr. CONDIT. Why don't you give a stab at it?

Ms. JACOBS. OK, a quick answer in the AIDS area is New York and California, which obviously have a huge percentage of the national population of affected persons. The New York HIV testing and disclosure law is stricter in its provisions for informed consent, in who may or may not get the information, and in the health use and the limitations, even within the health care setting, of the use.

Mr. HORN. Good. Those would be very helpful in terms of where are State laws stronger. I am just curious, with the 50 States, are there any others that would meet that test that you are talking about of being stronger laws?

Mr. CONDIT. It is our understanding—and, once again, I am not an expert on this—our best guess at this is that New York and California are the only two States that probably have stronger laws than what we are doing.

We can get whatever information is available to you, Mr. Horn.

Mr. HORN. Fine.

Mr. CONDIT. If we go out and do it separately, I have been told that we are looking at possibly 4, 5, 6 months to accumulate all the information on our own, but we have the information and if you are satisfied with that, once you look at it, that would save us a lot of time. If you are not, then we will have to sit down and try to figure out something else.

Ms. BERENSON. I would just also like to make the point that we need to be careful about comparing apples and oranges. This bill provides a much more comprehensive type of protection. It protects information in a number of settings, information that is in the control of a number of people.

I believe that there are a number of State laws that protect, for example, the fact of an HIV-positive test result and, in some States, that protection and the requirements regarding what you have to do before you can disclose that information are stronger than what you would need to do under this law, under H.R. 4077. On the other hand, those State protections may only apply in the health care provider setting and not in the insurer setting.

There are aspects of current State laws which I believe are much stronger in terms of, for example, what is disclosable and yet H.R. 4077 may be stronger in terms of defining the overall categories of those who have that information and who have a duty to somehow protect it.

Mr. CONDIT. Good point. Why don't we try to do that, if that is OK?

Mr. HORN. Sure.

Mr. CONDIT. We have the information and Mr. Gellman will get it to you, and you can review it.

Mr. HORN. Fine.

Mr. CONDIT. If you are unhappy with that, then we can come back and try to do something else, if it is possible to do. Do you have some additional questions?

Mr. HORN. Yes. I will not be asking for you, so you are free here. [Laughter.]

That one was one that I wanted to get straight.

Mr. CONDIT. I will be right back.

Mr. HORN. To what extent should the Federal Government's role be requiring informed consent? What is your belief on that, just to get it in one place at one time?

Ms. GOLDMAN. Informed consent is one of the absolutely critical areas in health care. What this bill does is talk about informed consent in terms of the use of information.

This bill does not address informed consent procedures for treatment.

H.R. 4077 does address informed consent for disclosure and use of information in a very comprehensive and very strong way, except for the one suggestion that I made about disclosure to next of kin. In order to have informed consent in that people must be notified of their right to object to the disclosure; but I think that this bill does a very strong job in that area.

Mr. HORN. Again, the ACLU, it seems to me, has a record here of fighting for the individual. Is that not correct?

Ms. GOLDMAN. That is correct, sir.

Mr. HORN. We now have two individuals. What if that individual does not release the records? Have we thought about the harm that can happen to another individual?

Ms. GOLDMAN. I know that this is a concern of yours. We are not rewriting public health law in H.R. 4077. Public health authorities are still able to use information and disclose information in legally authorized ways.

If the States have determined that public health authorities should be gathering information or disclosing information for exactly the purposes that you have been discussing, this bill does not touch that authority. In fact, most public health authorities in the States have pretty substantial reporting and notification responsibilities. That is not affected by this legislation.

Mr. HORN. Do you have anywhere a study the ACLU has made on that very issue as to what the State law is on informed consent?

Ms. GOLDMAN. Yes, we do, absolutely.

Mr. HORN. Could we have that as part of the record?

Ms. GOLDMAN. We have a study that the ACLU has done, for instance, on informed consent as it affects other individuals, as it would affect, for instance, spouses or partners. I would be very happy to provide for you.

Mr. HORN. Fine. If we might get it included in the record, I would like to see that included.

[The information follows:]

June 7, 1994

The Honorable Stephen Horn
1023 Longworth House Office Building
Washington, D.C. 20515

Dear Congressman Horn:

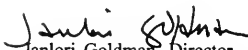
In response to questions you posed at the hearings held recently on health information privacy by the Government Operations Subcommittee on Information, we are sending you our views on the relationship between the Fair Health Information Practices Act (H.R. 4077) and state laws regarding partner notification.


If states wish to receive funds disbursed by the Centers for Disease Control (CDC) for HIV testing, they must have in place a system for the notification of spouses or partners of HIV-infected individuals. All states currently receive funds under this program, termed the Counseling, Testing, Referral, and Partner Notification Program. As a condition of receiving funds, states must certify they have a partner notification system in place, pursuant to state law or regulation.

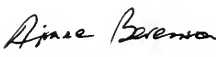
H.R. 4077 is not intended to supersede these state laws or regulations. Indeed, it is our understanding that the bill will allow such notifications to continue to occur, consistent with the procedures established by the various states.


We hope this answers your question. Feel free to contact any of us if you have any further concerns.

Sincerely,


Janlori Goldman, Director
Privacy and Technology Project
Electronic Frontier Foundation
202-347-5400


Chai Feldblum, Director
Federal Legislation Clinic
Georgetown University Law Center
202-662-9595

 (CEF)
Aimee Berenson
AIDS Action Council
202-986-1300 ext. 24

 (CEF)
Susan Jacobs
Legal Action Center
212-243-1313

Ms. BERENSON. Also, may I just address that question?

Mr. HORN. Sure.

Ms. BERENSON. I would point out that, in addition to what my colleague has just mentioned about the public health protections that are maintained in this bill, there is also a provision for emergency circumstances and there are provisions in this bill that would maintain current Federal provisions regarding notification of emergency workers, for example, who may have been exposed to blood-borne or air-borne diseases.

I understand your concern. I think there are a number of places in this bill where we have protected existing laws and provided for the kind of situation that you are so rightfully concerned about.

Mr. HORN. Thank you. Any comment, Ms. Jacobs, on that?

Ms. JACOBS. No, except to say I think Ms. Goldman's point is the important point here—well, not that yours is not, too, I'm sorry—that we are in a sense, as you had said, talking apples and oranges.

One is a privacy bill and it does not—your bill does not, in any way, usurp public health functions. Informed consent, whether written or oral informed consent, is only about a piece of disclosure of information.

Mr. HORN. OK. Now, with regard to the penalties included in H.R. 4077, should the individual responsible for breaching the information be held accountable or should the institution be held accountable? This gets back to a question I have asked two previous panels, of the so-called disgruntled employee.

As you know, our first witness the first day of these hearings was a colleague in the House, where confidential information was breached and attempted to be used against her in a political campaign.

You have the problem with large institutions, HMO's, hospitals, any form of organized medicine you and I can think of, where there are a lot of files, there are a lot of people with access, and one never knows what some employees might do. 99.9 percent are loyal. A few go out and decide they are going to have a grudge and get even with the employer.

Having headed an institution of 4,200 employees, I can assure you that happens in a university, it happens in a hospital, it happens in government, in happens in any corporation or business.

How do we deal with that when the institution might well have everything from signing your name to get a record and so forth and, suddenly, years later, a Xerox—which is easy to get any time, night or day, in most organizations—of this confidential file is dumped before a newspaper, a TV station, or in the middle of a political campaign?

What is your feeling on the role, then, of dealing with that individual that dumped it; or do we deal with the institution out of whose files that information was stolen?

Ms. GOLDMAN. I am glad you are asking that question of this panel because I have heard you ask it before and it is a very important question.

Employers or institutions should be liable for the actions of their employees. When there is liability on the institution, the institution will try to guard against breaches.

There are many hospitals right now where it is not so easy to get personal health information. As Kathleen Frawley testified yesterday, there are hospitals that have extremely strict rules regarding who can have access to somebody's health record and under what circumstances.

They have put in audit trails so they know who has seen information. They know who has had access to the information and for what reason so, in the event there is a breach, they can then go back and look at who has had access to that information.

The executive branch would do well to do the same thing. We have had some unauthorized disclosures of information from the Social Security Administration, from the IRS, and it is important to put in place some kind of a security mechanism.

As to the question of who is liable, in this circumstance, it should be both the individual, if we can find out who that is—and in Congresswoman Velázquez's case, that is not clear—and it should also be the institution whose job it is, whose obligation it is, to guard that information.

When somebody seeks treatment in a hospital, they should not have to make the decision, "Should I seek treatment or should I not because I am worried about confidentiality?" They should know that their interest is protected, regardless of whether you can find out who breached the confidentiality or you cannot.

I think that you will find that institutions will become even more responsible than most of them already are if they are liable for the actions of their employees, as most institutions are where there is a law in place. There are very few institutions that are shielded from liability for breaches caused by a disgruntled employee. They are responsible for that person's actions and I think they should be.

Mr. HORN. I go back to my senior colleagues' example of Greybull, WY this morning. I am not sure how many people live there. I have been through Wyoming. Not many people live there, generally.

I happened to grow up on a ranch 5 miles from San Juan Bautista, CA—no doctor in San Juan Bautista; nearest doctor 10 miles in Gilroy, 13 miles in Hollister.

The Hazel Hawkins Memorial Hospital in Hollister, CA, I doubt can have a 24-hour-a-day guard of the records and, at 2 a.m., where the one emergency of the month might occur, the question is, who gets into those records? The medical staff obviously might need them—someone—and who is the guardian watching the guardian, to go back to Plato a little bit?

Your answers seem to presume some huge bureaucracy where we have the security of files task force vigilantly sitting there night and day to make sure we have a signature when that file goes out but, in a big, urban hospital, I would think—and I would bet you numerous security tests would prove this point—there is no way you can secure those records, no matter how hard you try.

You are saying, "OK, let's file a suit against the institution." Why not file a suit against the individual that violated the security?

Ms. GOLDMAN. Mr. Congressman, I could not agree with you more. We should file a suit against the individual when we know who it is that has breached the person's confidentiality. As Con-

gresswoman Velázquez said when she testified, it is not always clear who that individual is.

I am not saying that institutions will become perfect in their security or that every institution is a large bureaucracy. Excuse me if that was the impression that I created.

If there is a law which will make institutions liable for breaches, they will become much better at protecting information, whether it is a two-person institution or a 20,000-person institution. There are mechanisms, both technical and other, that can protect information to a greater extent than currently provided.

There is no 100 percent foolproof system. However, I think that we can do better than we are doing now.

Mr. HORN. Should we make it a felony if there is a violation of the security provisions of this act?

Ms. GOLDMAN. If there is a violation of a security provision but there has not been a harm to an individual resulting from that violation, then no, the violation should not be a felony.

Mr. HORN. Let us say there has been harm to the individual. Should these simply be civil damages? Should this be criminal action on the part of the Federal Government?

Ms. JACOBS. There is precedent, for instance, again, in the drug-alcohol law, for possible criminal investigations based on breaches of security or violations of confidentiality. I do agree, though, it depends, as you know, on showing the intent and being able to nail down the individual person.

I also wanted to add that we do trainings nationally and, while I have not been in Wyoming yet, I was in Reading, CA not that long ago and spoke with a group of people from a very small clinic in a rural area.

One of the things that are all facing is something I think this act is addressing well—is the electronic transfer of information so information that did not used to be able to be circulated and where maybe you did need a guard at the door, no longer requires that any more for certain kinds of disclosures.

Mr. HORN. Right. You are right. It is very difficult to trace, even where is it, who has it. Any other comments on that particular point? Ms. Berenson.

Ms. BERENSON. I agree with what my colleagues have said and—I would just reiterate that with regard to an institution's liability, they are only liable if they have breached a standard of care.

I do not think that it is unreasonable or unduly burdensome to require that there be a basic standard of care and a duty to maintain that standard of care with regard to the confidentiality of medical records.

Mr. HORN. Again, I would ask you to think of the small clinic, small hospitals of America where it is hard to even keep the doors open sometimes.

Ms. BERENSON. Many of the AIDS service organizations that are members of AIDS Action Council are in that position, and I have been impressed by the ingenuity and ease with which they have adapted to security measures. I think people are afraid of this idea, afraid of what it involves, and I think that, if they sit down and think about how they can go about protecting records, it is a very

useful and a very productive exercise and a successful one, even in very small organizations.

Ms. GOLDMAN. May I just make a final comment on this point?

Mr. HORN. Sure.

Ms. GOLDMAN. As this bill was moving through the drafting process, a number of us were very concerned that the associations and the institutions that would ultimately be liable under this bill would have serious objections against the liability provisions.

I think that it has been very encouraging that these institutions have not objected, that they accept these provisions as part of their responsibility, and that these provisions are not a dramatic departure from either what they are already having to comply with under State law or what they see as their duty in a confidentiality setting.

I have, as I said, found that very encouraging. I believe these institutions will take the steps to improve security and to train employees necessary to comply with the provisions of this bill.

Mr. HORN. I would agree with you, and large organizations should not have a problem complying. I am worrying a little about the small organizations.

Ms. GOLDMAN. I understand.

Mr. HORN. What is your assessment of the administration's proposal to create a national information system and regional data centers and will this information be secure and, if not, could the private sector be doing a better job?

Ms. JACOBS. I will take a stab at it. I am not a computer person but I have been talking to several. One of the things that is very impressive to me is that there is an ability to secure electronic data. You have acknowledged that in the act. What I am told is people do not utilize that ability, for a myriad of reasons, but that it is not all that difficult in some ways.

For instance, I talked with somebody about the objection people have to written pieces of paper. A question was asked to us about what are you going to do when there are no longer pieces of paper for anyone to sign and so, when you talk about written informed consent, you are talking about a signature and haven't you just lost that?

I was not sure, and talked to a computer friend, who said we can—I do not even know what the word is, but we take a picture of the document with the signature—it has a computer word—and, essentially, store that on a disk and then, when we need it, we recall it, so there is not a problem in, again, continuing to use signatures, continuing to use certain other security measures. I think there is an issue about willingness.

I will add to that that I think this committee has done a remarkable job in the wave of the tendency to information superhighway everything. I think it is good to step back and to say, "Wait a minute, let's look at what that really means in terms of privacy."

Mr. HORN. Any other comments on that point?

Ms. GOLDMAN. I want to address the specific concern you raised about whether the government or the private sector should be involved in the collection of personal health information. We have not taken a formal position on this but I wanted to raise a possible concern.

The regional health data centers that are envisioned by the administration, and are already being created at State and local level around the country will hold sensitive and personal information gathered from providers and employers, in the research context, in the payment context, possibly even in the marketing context. There would be a great concern on the part of the American public if it were the government that was the ultimate repository for all of this information.

Not that we could not put laws in place that would restrict their use of the information. We can do that. However, in the future, those laws could be weakened. I think that there would be a tremendous temptation on the part of government agencies to use that information for other purposes.

We have seen that time and again with the creation of information by the government, whether it was for Social Security purposes, tax purposes, or immigration purposes, criminal history records or data bases created for a limited purpose. A temptation to use them for other purposes was irresistible and the laws that created those information systems were undermined and weakened in ways that I think had very substantial impact on individual liberties.

That is the only caveat that I raise in terms of who should be the ultimate controller or compiler of this information. The public would be extremely suspicious, and they are extremely suspicious, when they hear talk about an electronic data network as is envisioned by the Health Security Act proposed by the administration. This is something we need to be very careful about.

Mr. HORN. I think you make an excellent point. In other words, what you are saying is, if we can, let us decentralize information to the need. It is sort of the presumed but not always followed—maybe not in the majority followed—the “need to know,” rather than simply getting this where anybody can access that has the magic code number.

Ms. GOLDMAN. Absolutely.

Ms. BERENSON. I would just like to give a slightly different perspective on what my colleague was saying with regard to the government versus the private sector.

In the AIDS context, it has been very interesting. Until now, most of our concern has focused on this issue of providing information to public authorities for public health purposes, and we have had situations where there were attempts to access the information that those governmental entities had for purposes that were clearly improper.

However, the reality, if you look at the caselaw, has been that most of the misuses of information with regard to HIV and AIDS have occurred in the private sector. There are very strong financial incentives in the private sector to misuse information about people's personal health status, which I think really need to be taken into consideration with regard to whether the private sector is the appropriate place to be placing huge data banks of information or whether the private sector should have access to those data banks.

As much as we may be concerned about government, at least when government does something, we can scream about it and we know what they are doing. I have great concerns that, in the pri-

vate sector, our experience has been, all too often, that lists are sold to marketers and researchers and used for all kinds of purposes that should not have been approved, because nobody was aware of how that information was being handled in the private sector.

Mr. CONDIT. Mr. Horn, may I just follow up?

Mr. HORN. Sure.

Mr. CONDIT. Is that because there were no standards or rules or regulations for the private sector to follow?

Ms. BERENSON. I certainly think that that is a big part of it. Of course, the issue of standards for the private sector to follow is very important, but additionally there has to then be clear enforcement of those standards.

Who is enforcing those standards? There should be private cause of action but, additionally, there needs to be some government oversight and enforcement of those standards and systems as well to ensure that the protections that we build in are not just paper protections.

Mr. CONDIT. Is it not true if we do not have standards and rules for the private sector or the government, you can abuse this?

Ms. BERENSON. Of course.

Mr. CONDIT. Whoever we give this responsibility to, we have to have rules and standards and penalties for violating them.

Ms. BERENSON. That is right.

Mr. CONDIT. We can debate whether it should be the private sector or the government. I have my own personal preference. It may be that we can prove that one is better than the other but, still, we have to have standards or rules or we have missed the mark.

Mr. Horn.

Mr. HORN. I have just a question, Mr. Chairman. You might be able to remind me. Your bill does protect us from, say, some groups selling lists based on disease—

Mr. CONDIT. Yes.

Mr. HORN [continuing]. In terms of newsletters, magazines, so forth, as I recall.

Mr. CONDIT. Right.

Mr. HORN. That would certainly be a typical way for somebody to try to make a buck out of a medical and health file.

Mr. CONDIT. We have asked the private sector to comment on every step of that and they have been supportive of us setting the standards.

Also—just to follow up on a comment that you made about the liability question—yesterday we had the American Hospital Association, and they have divisions of that association which represent rural and city hospitals. They were very supportive of taking the responsibility on themselves. They did not balk at this at all. We have stayed in touch with them every step of the way.

I have asked Mr. Gellman, though—there is a group called Rural Hospital Association—and we will make contact with them and ask them for their input. I think it would be appropriate to do that.

Mr. HORN. I thank the witnesses for their testimony. It has been immensely helpful.

Mr. CONDIT. Mrs. Thurman.

[No response.]

Mr. CONDIT. I have some additional questions and I would like to submit those to you in writing. We are going to start here in a little bit, and we have a gun issue on the floor, so I would like to move on, if I can.

I want you to know that we appreciate very much your being here this morning. Your participation in this issue is important to the success of the issue and we want you to stay on board with us, try to work out the problems, and we will stay in touch with you. Thank you very much.

[Whereupon, at 11 a.m., the subcommittee adjourned, to reconvene subject to the call of the Chair.]

A P P E N D I X E S

APPENDIX 1.—RESPONSE TO SUBCOMMITTEE QUESTIONS BY MS. PATTI GOLDMAN, SENIOR ASSOCIATE DIRECTOR, CONGRESSIONAL AND EXECUTIVE BRANCH RELATIONS, AMERICAN HOSPITAL ASSOCIATION

American Hospital Association



Capitol Place, Building #3
50 F Street, N.W.
Suite 1100
Washington, D.C. 20001
Telephone 202.638-1100
FAX NO 202.626-2345

December 22, 1993

Representative Gary Condit
Chairman
Subcommittee on Information, Justice,
Transportation and Agriculture
Committee on Government Operations
U. S. House of Representatives
B349-C Rayburn House Office Building
Washington, D. C. 20515

Dear Mr. Condit:

We have received the additional questions submitted after the November 4, 1993 hearing on confidentiality of patient information. I am pleased to be able to submit the following answers, while cautioning that the American Hospital Association (AHA) can only speak for hospitals in general, and cannot speak for any one hospital in particular. Moreover, in answering Question 1, we can only provide material from the American Hospital Association, and not from any other professional hospital organizations.

Question # 1 -- Does the AHA or other professional hospital association have any rules, guidelines, or ethical principles on the use of identifiable patient information for marketing? If so, please provide a copy.

The AHA has no specific guidelines on the use of patient information for marketing purposes, but I am attaching to this letter copies of AHA Management Advisories on "Advertising by Health Care Facilities," "Ethical Conduct for Health Care Institutions," "A Patient's Bill of Rights," and "Disclosure of Medical Record Information," as well as a copy of AHA's "General Guide for the Release of Patient Information by the Hospital." Throughout AHA publications, guidelines, and advisories, the general issue of patient confidentiality is given paramount importance.

Question # 2 -- Is there any general information available on the scope of hospital marketing activities based on identifiable patient information? Copies of marketing plans, journal articles, and similar items would be helpful in describing these activities.

Identifiable patient information is typically not used in marketing activities. Aggregate data is usually what is most valuable to marketers.

Question # 3 -- Do hospitals use identifiable patient information as a basis for marketing goods or services? If possible, provide specific examples of marketing activities.

Hospitals typically do not use identifiable patient information as a basis for marketing. They use aggregate data, payor statistics, utilization review data, patient origin data, and other types of demographic data. This kind of data yields trends, which are preferable to details in marketing.

Question # 4 -- Do hospitals use identifiable patient information as the basis for patient questionnaires or satisfaction surveys? If so, please describe the manner in which these activities are conducted. If any information is shared with outside organizations, please describe the terms under which that information may be used.

Yes. Hospitals routinely survey discharged patients, usually by mail, to assess patient satisfaction, identify problems, etc. This information is part of any good Total Quality Management/Continuous Quality Improvement process. Patient-specific information is not factored into the selection of those randomly surveyed. Deceased patients are, however, removed from the lists before names are selected. This information can be shared or managed by an outside market research company for execution and analysis, but specific patient information (such as specifics about diagnosis or treatment) are not provided to the researchers.

Some hospitals also use patients in advertisements. When this is done, it is done with the patient's full permission and cooperation, observing all legalities.

Question # 5 -- Do hospitals disclose, sell, or otherwise share mailing lists of patients with other institutions, including other hospitals? If so, please describe.

No.

Question # 6 -- Do hospitals disclose, sell, or otherwise share identifiable patient prescription information with drug or equipment manufacturers or vendors?

No.

Question # 7 -- Do hospitals share identifiable patient information with affiliated organizations or companies? If so, please describe.

This sharing of information sometimes occurs, at the request of the patient, in the process of discharge planning. For example, a patient may request to be signed up for a Meals on Wheels program upon discharge from the hospital. It also may be done with the patient's knowledge and approval as in the case of an obstetrical short-stay program where the hospital arranges for a home health care aide to visit the patient 24 hours after discharge.

Question # 8 -- Do hospitals allow the use of identifiable patient information for fund raising activities? If so, please describe.

Yes. Hospitals frequently use lists of discharged patients for fundraising purposes.

Question # 9 -- Do hospitals disclose, sell, or otherwise share lists of expectant mothers, new births, or recently deceased patients?

Hospitals don't typically release this information. It is important to point out that in many cases this information is part of the public record, and is therefore readily available to the media and other sources. Hospitals are required by state law(s) to report this information to various public authorities. Moreover, public hospitals have specific public disclosure requirements.

I hope these answers provide you and the subcommittee with the information you need. Please feel free to contact me at 626.2328 if I can provide any further material.

Sincerely,



Patti Roberts Goldman
Senior Associate Director
Congressional and Executive Branch Relations

Enc.

*A Patient's Bill of Rights*PATIENT AND
COMMUNITY RELATIONS

Introduction

Effective health care requires collaboration between patients and physicians and other health care professionals. Open and honest communication, respect for personal and professional values, and sensitivity to differences are integral to optimal patient care. As the setting for the provision of health services, hospitals must provide a foundation for understanding and respecting the rights and responsibilities of patients, their families, physicians, and other caregivers. Hospitals must ensure a health care ethic that respects the role of patients in decision making about treatment choices and other aspects of their care. Hospitals must be sensitive to cultural, racial, linguistic, religious, age, gender, and other differences as well as the needs of persons with disabilities.

The American Hospital Association presents *A Patient's Bill of Rights* with the expectation that it will contribute to more effective patient care and be supported by the hospital on behalf of the institution, its medical staff, employees, and patients. The American Hospital Association encourages health care institutions to tailor this bill of rights to their patient community by translating and/or simplifying the language of this bill of rights as may be necessary to ensure that patients and their families understand their rights and responsibilities.

Bill of Rights*

1. The patient has the right to considerate and respectful care.
2. The patient has the right to and is encouraged to obtain from physicians and other direct caregivers relevant, current, and understandable information concerning diagnosis, treatment, and prognosis.

Except in emergencies when the patient lacks decision-making capacity and the need for treatment is urgent, the patient is entitled to the opportunity to discuss and request information related to the specific procedures and/or treatments, the risks involved, the possible length of recuperation, and the medically reasonable alternatives and their accompanying risks and benefits.

Patients have the right to know the identity of physicians, nurses, and others involved in their care, as well as when those involved are students, residents, or other trainees. The patient also has the right to know the immediate and long-term financial implications of treatment choices, insofar as they are known.

3. The patient has the right to make decisions about the plan of care prior to and during the course of treatment and to refuse a recommended treatment or plan of care to the extent permitted by law and hospital policy and to be informed of the medical consequences of this action. In case of

such refusal, the patient is entitled to other appropriate care and services that the hospital provides or transfer to another hospital. The hospital should notify patients of any policy that might affect patient choice within the institution.

4. The patient has the right to have an advance directive (such as a living will, health care proxy, or durable power of attorney for health care) concerning treatment or designating a surrogate decision maker with the expectation that the hospital will honor the intent of that directive to the extent permitted by law and hospital policy.

Health care institutions must advise patients of their rights under state law and hospital policy to make informed medical choices, ask if the patient has an advance directive, and include that information in patient records. The patient has the right to timely information about hospital policy that may limit its ability to implement fully a legally valid advance directive.

5. The patient has the right to every consideration of privacy. Case discussion, consultation, examination, and treatment should be conducted so as to protect each patient's privacy.

*These rights can be exercised on the patient's behalf by a designated surrogate or proxy decision maker if the patient lacks decision-making capacity, is legally incompetent, or is a minor.



A Patient's Bill of Rights was first adopted by the American Hospital Association in 1973. This revision was approved by the AHA Board of Trustees on October 21, 1992.

© 1992 by the American Hospital Association, 840 North Lake Shore Drive, Chicago, Illinois 60611. Printed in the U.S.A. All rights reserved. Catalog no. 137759.

6. The patient has the right to expect that all communications and records pertaining to his/her care will be treated as confidential by the hospital, except in cases such as suspected abuse and public health hazards when reporting is permitted or required by law. The patient has the right to expect that the hospital will emphasize the confidentiality of this information when it releases it to any other parties entitled to review information in these records.
7. The patient has the right to review the records pertaining to his/her medical care and to have the information explained or interpreted as necessary, except when restricted by law.
8. The patient has the right to expect that, within its capacity and policies, a hospital will make reasonable response to the request of a patient for appropriate and medically indicated care and services. The hospital must provide evaluation, service, and/or referral as indicated by the urgency of the case. When medically appropriate and legally permissible, or when a patient has so requested, a patient may be transferred to another facility. The institution to which the patient is to be transferred must first have accepted the patient for transfer. The patient must also have the benefit of complete information and explanation concerning the need for, risks, benefits, and alternatives to such a transfer.
9. The patient has the right to ask and be informed of the existence of business relationships among the hospital, educational institutions, other health care providers, or payers that may influence the patient's treatment and care.
10. The patient has the right to consent to or decline to participate in proposed research studies or human experimentation affecting care and treatment or requiring direct patient involvement, and to have those studies fully explained prior to consent. A patient who declines to participate in research or experimentation is entitled to the most effective care that the hospital can otherwise provide.
11. The patient has the right to expect reasonable continuity of care when appropriate and to be informed by physicians and other caregivers of available and realistic patient care options when hospital care is no longer appropriate.
12. The patient has the right to be informed of hospital policies and practices that relate to patient care, treatment, and responsibilities. The patient has the right to be informed of available resources for resolving disputes, grievances, and conflicts, such as ethics committees, patient representatives, or other mechanisms available in the institution. The patient has the right to be informed of the hospital's charges for services and available payment methods.

The collaborative nature of health care requires that patients, or their families/surrogates, participate in their care. The effectiveness of care and patient satisfaction with the course of treatment depend, in part, on the patient fulfilling certain responsibilities. Patients are responsible for providing information about past illnesses, hospitalizations, medications, and other matters related to health status. To participate effectively in decision making, patients must be encouraged to take responsibility

for requesting additional information or clarification about their health status or treatment when they do not fully understand information and instructions. Patients are also responsible for ensuring that the health care institution has a copy of their written advance directive if they have one. Patients are responsible for informing their physicians and other caregivers if they anticipate problems in following prescribed treatment.

Patients should also be aware of the hospital's obligation to be reasonably efficient and equitable in providing care to other patients and the community. The hospital's rules and regulations are designed to help the hospital meet this obligation. Patients and their families are responsible for making reasonable accommodations to the needs of the hospital, other patients, medical staff, and hospital employees. Patients are responsible for providing necessary information for insurance claims and for working with the hospital to make payment arrangements, when necessary.

A person's health depends on much more than health care services. Patients are responsible for recognizing the impact of their life-style on their personal health.

Conclusion

Hospitals have many functions to perform, including the enhancement of health status, health promotion, and the prevention and treatment of injury and disease; the immediate and ongoing care and rehabilitation of patients; the education of health professionals, patients, and the community; and research. All these activities must be conducted with an overriding concern for the values and dignity of patients.

responsibilities of their employees and medical staff members and be sensitive to institutional decisions that employees might interpret as compromising their ability to provide high-quality health care.

- Health care institutions should provide for fair and equitably-administered employee compensation, benefits, and other policies and practices.
- To the extent possible and consistent with the ethical commitments of the institution, health care institutions should accommodate the desires of employees and medical staff to embody religious and/or moral values in their professional activities.
- Health care institutions should have written policies on conflict of interest that apply to officers, governing board members, and medical staff, as well as others who may make or influence decisions for or on behalf of the institution, including contract employees. Particular attention should be given to potential conflicts related to referral sources, vendors, competing health care services, and investments. These policies should recognize that individuals in decision-making or administrative positions often have duality of interests that may not always present conflicts. But they should provide mechanisms for identifying and addressing dualities when they do exist.
- Health care institutions should communicate their mission, values, and priorities to their employees and volunteers, whose patient care and service activities are the most visible embodiment of the institution's ethical commitments and values.

AHA Resources

The American Hospital Association developed its first "code of ethics" for health care institutions called *Guidelines on Ethical Conduct and Relationships for Health Care Institutions* in 1973 as a complement to the code of ethics for hospital executives (available from the American College of Healthcare Executives). This management advisory is the most current version of this code. The AHA and its members are committed to regular review and updating of this advisory to assure that it is responsive to contemporary ethical issues facing health care institutions.

This advisory identifies the major areas affecting the ethical conduct of health care institutions. It would be impossible for one advisory document to detail all of the factors and issues relating to each area. Additional information and guidance is available in the following AHA management advisories:

A Patient's Bill of Rights

Advertising

Discharge Planning

Disclosure of Financial and Operating Information

Disclosure of Medical Record Information

Establishment of an Employee Grievance Procedure

Ethics Committees

Imperatives of Hospital Leadership

Physician Involvement in Governance

Quality Management

Resolution of Conflicts of Interest

The Patient's Choice of Treatment Options

Verifying Physician Credentials

Verifying Credentials of Medical Students and Residents

The following AHA publications may also be useful:

Values in Conflict: Resolving Ethical Issues in Hospital Care (AHA #025002)

Effective DNR Policies: Development, Revision, and Implementation (AHA #058750)

Hospital Ethics newsletter

*Ethical Conduct for
Health Care Institutions***Introduction**

Health care institutions,* by virtue of their roles as health care providers, employers, and community health resources, have special responsibilities for ethical conduct and ethical practices that go beyond meeting minimum legal and regulatory standards. Their broad range of patient care, education, public health, social service, and business functions is essential to the health and well being of their communities. These roles and functions demand that health care organizations conduct themselves in an ethical manner that emphasizes a basic community service orientation and justifies the public trust. The health care institution's mission and values should be embodied in all its programs, services, and activities.

Because health care organizations must frequently seek a balance among the interests and values of individuals, the institution, and society, they often face ethical dilemmas in meeting the needs of their patients and their communities. This advisory is intended to assist members of the American Hospital Association to better identify and understand the ethical aspects and implications of institutional policies and practices. It is offered with the understanding that each institution's leadership in making policy and decisions must take into account the needs and values of the institution, its physicians, other caregivers, and

employees and those of individual patients, their families, and the community as a whole.

The governing board of the institution is responsible for establishing and periodically evaluating the ethical standards that guide institutional policies and practices. The governing board must also assure that its own policies, practices, and members comply with both legal and ethical standards of behavior. The chief executive officer is responsible for assuring that hospital medical staff, employees, and volunteers and auxiliaries understand and adhere to these standards and for promoting a hospital environment sensitive to differing values and conducive to ethical behavior.

This advisory examines the hospital's ethical responsibilities to its community and patients as well as those deriving from its organizational roles as employer and business entity. Although explicit responsibilities also are included in legal and accreditation requirements, it should be remembered that legal, accreditation, and ethical obligations often overlap and that ethical obligations often extend beyond legal and accreditation requirements.

Community Role

- Health care institutions should be concerned with the overall health status of their communities while continuing to provide direct patient services. They should

take a leadership role in enhancing public health and continuity of care in the community by communicating and working with other health care and social agencies to improve the availability and provision of health promotion, education, and patient care services.

- Health care institutions are responsible for fair and effective use of available health care delivery resources to promote access to comprehensive and affordable health care services of high quality. This responsibility extends beyond the resources of the given institution to include efforts to coordinate with other health care organizations and professionals and to share in community solutions for providing care for the medically indigent and others in need of specific health services.
- All health care institutions are responsible for meeting community service obligations which may include special initiatives for care for the poor and uninsured, provision of needed medical or

**The term "health care institution" represents the mission, programs, and services as defined and implemented by the institution's leadership, including the governing board, executive management, and medical staff leadership. See also management advisories on Imperatives of Hospital Leadership, Role and Functions of Hospital Executive Management, Role and Functions of the Hospital Governing Board, and Role and Functions of the Hospital Medical Staff.*

This advisory was revised by the AHA Technical Panel on Biomedical Ethics and approved by the Institutional Practices Committee in 1992.

© 1992 by the American Hospital Association, 640 North Lake Shore Drive, Chicago, Illinois 60611.
Printed in the U.S.A. All rights reserved. Order #049722

social services, education, and various programs designed to meet the specific needs of their communities.

- Health care institutions, being dependent upon community confidence and support, are accountable to the public, and therefore their communications and disclosure of information and data related to the institution should be clear, accurate, and sufficiently complete to assure that it is not misleading. Such disclosure should be aimed primarily at better public understanding of health issues, the services available to prevent and treat illness, and patient rights and responsibilities relating to health care decisions.
- Advertising may be used to advance the health care organization's goals and objectives and should, in all cases, support the mission of the health care organization. Advertising may be used to educate the public, to report to the community, to increase awareness of available services, to increase support for the organization, and to recruit employees. Health care advertising should be truthful, fair, accurate, complete, and sensitive to the health care needs of the public. False or misleading statements, or statements that might lead the uninformed to draw false conclusions about the health care facility, its competitors, or other health care providers are unacceptable and unethical.*
- As health care institutions operate in an increasingly challenging environment, they should consider the overall welfare of their communities and their own missions in determining their activities, service mixes, and business. Health care organizations should be particularly sensitive to potential conflicts of

interests involving individuals or groups associated with the medical staff, governing board, or executive management. Examples of such conflicts include ownership or other financial interests in competing provider organizations or groups contracting with the health care institution.

Patient Care

- Health care institutions are responsible for providing each patient with care that is both appropriate and necessary for the patient's condition. Development and maintenance of organized programs for utilization review and quality improvement and of procedures to verify the credentials of physicians and other health professionals are basic to this obligation.
- Health care institutions in conjunction with attending physicians are responsible for assuring reasonable continuity of care and for informing patients of patient care alternatives when acute care is no longer needed.
- Health care institutions should ensure that the health care professionals and organizations with which they are formally or informally affiliated have appropriate credentials and/or accreditation and participate in organized programs to assess and assure continuous improvement in quality of care.
- Health care institutions should have policies and practices that assure that patient transfers are medically appropriate and legally permissible. Health care institutions should inform patients of the need for and alternatives to such transfers.

- Health care institutions should have policies and practices that support informed consent for diagnostic and therapeutic procedures and use of advance directives. Policies and practices must respect and promote the patient's responsibility for decision making.
- Health care institutions are responsible for assuring confidentiality of patient-specific information. They are responsible for providing safeguards to prevent unauthorized release of information and establishing procedures for authorizing release of data.
- Health care institutions should assure that the psychological, social, spiritual, and physical needs and cultural beliefs and practices of patients and families are respected and should promote employee and medical staff sensitivity to the full range of such needs and practices. The religious and social beliefs and customs of patients should be accommodated whenever possible.
- Health care institutions should have specific mechanisms or procedures to resolve conflicting values and ethical dilemmas as well as complaints and disputes among patients/their families, medical staff, employees, the institution, and the community.

Organizational Conduct

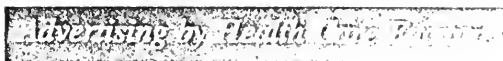
- The policies and practices of health care institutions should respect and support the professional ethical codes** and

*Adopted from the AHA Management Advisory on Advertising, 1990.

**For example, the American College of Healthcare Executives' Code of Ethics, and professional codes of nursing, medicine, etc.

MANAGEMENT
ADVISORY

PATIENT AND
COMMUNITY RELATIONS



Introduction

Advertising is commonly used by hospitals and other health care facilities to communicate with patients, potential patients, and other constituent groups. Because of the unique relationship between health care organizations and the people they serve, these guidelines are suggested to ensure that health care organizations implement their advertising with fairness, honesty, accuracy, and sensitivity to the special trust that exists between patients and health care providers.

The American Hospital Association first approved guidelines for advertising by hospitals in August 1977. In that document, references were made to the importance of communication between hospitals and their publics, and the significant and appropriate role that advertising may have in that communication process.

Advertising, like all methods of communication, should be used to advance the health care providers' goals and objectives and should, in all cases, support the mission of the health care organization.

Advertising seeks to persuade, generate a response, or facilitate a business exchange. For the purpose of these guidelines, advertising includes, but is not necessarily limited to, display ads in newspapers, billboards, recruitment notices, radio and television ads, brochures, advertising in telephone directories, direct mail, and all

similar forms of promotional communications.

These guidelines are intended to define a number of common purposes of advertising and to comment upon the content of health care advertising efforts.

Purposes of Health Care Advertising
Public Education about Available Services

It is in the best interest of the public to be informed of the availability and the attributes of services that may have a significant influence on health. Advertising can help make such services known to the public and encourage the appropriate utilization of these services.

Public Education about Health Care

Health promotion and illness prevention are important elements of health care. Services and programs that attempt to assist the public in maintaining health are offered by many health care facilities. Advertising is often used in conjunction with this education effort, either to inform or to encourage participation. Such advertising can demonstrate the health care facility's concern about public health or encourage appropriate utilization of health and wellness facilities and services.

Public Accountability

Health care organizations are expected to be accountable to their public constituencies. Advertising that is used to make a public report or inform the public about the organization's activities, challenges, financial position, or future plans, can be helpful in meeting public expectations.

Maintain or Increase Market Share

In an increasingly competitive and cost-conscious environment, health care organizations often use advertising to help maintain or attempt to increase market share for specific services and programs. Such advertising can result in the efficient, appropriate and cost-effective use of services to benefit both the consumer and the health care facility.

Public Support

Health care organizations frequently use advertising to enhance fundraising campaigns. Advertising can also be used to affect public support of social, civic or political issues. However, advertising to communicate a political point of view can raise serious questions concerning a health facility's tax status and should be carefully reviewed by legal counsel. Coordination of such advertising with local, state, and national



Approved by the Institutional Practices Committee in 1990, this document was revised by the American Society for Health Care Marketing and Public Relations.

© 1990 by the American Hospital Association, 840 North Lake Shore Drive, Chicago, Illinois 60611.
Printed in the U.S.A. All rights reserved. Catalogue no. 157760

hospital organizations is recommended.

Employee Recruitment

Advertising is a well-established and accepted means of recruiting necessary health care personnel to staff services and facilities.

Medical Staff Support

Advertising may be used to inform the public about the availability of services provided by a health care facility's medical staff. Advertising prepared in consultation with medical staff members may also be helpful in publicizing the capabilities of specific members of the medical staff. This type of advertising frequently is used to maintain or increase a health care facility's market share in a specific service.

Advertising in support of medical staff services may take the form of referral programs, which are designed to introduce new patients to members of the medical staff. Referral services that give the public informed choice and control over the selection of physician, and seek to match the public with physicians of appropriate training and capabilities, can benefit the consumer, the medical community and the health care facility. Criteria for participation in referral services should be fully disclosed.

Content of Health Care Advertising

The content of health care advertising must be measured primarily by its truthfulness, fairness, accuracy, completeness, and sensitivity to the health care needs of the public. False or misleading statements, or statements that might lead the uninformed to draw false conclu-

sions about the health care facility, its competitors, or other health care providers are unacceptable and unethical.

As with all health care services, advertising must be crafted and executed in the spirit of putting the needs of the patient first.

Health care advertising that promotes the use of excessive, unnecessary, or non-medically indicated health care services is unethical. Furthermore, advertising that encourages a health care consumer to take unreasonable risks, without disclosing the nature of the risks, is also unethical.

Advertising that targets the ill, infirm, frightened or other vulnerable groups, such as AIDS patients or patients diagnosed with cancer, requires special sensitivity and must meet the highest ethical standards. Patients who are ill or diagnosed with a severe disease may be desperate and in a state of mind incompatible with making informed health care decisions.

Advertising by health care facilities should not raise unrealistic expectations. Communication of success rates, outcomes and other statistical evidences of quality should be done with great care and in the spirit of honesty, accuracy, and full disclosure. Words such as *safe*, *effective*, *painless*, and *best* should be used with great caution and not without verifiable, objectively-based substantiation. Advertising should avoid stating or implying a guarantee of successful outcome or of complete patient satisfaction, unless the advertiser has a reasonable basis for making such a claim.

Direct or implied comparisons between one health care facility and another should not be made unless they can be objectively measured and fully substantiated.

Because comparative advertising involves a high risk of legal exposure, it may be appropriate to have such advertising reviewed by legal counsel.

Advertising that communicates cost information should be accurate, substantiated, and offered in the spirit of full disclosure. Advertising communicating a low initial cost is unethical where there is a reasonable probability of incurring additional costs later. Promotion of low-cost services, such as health screenings, that lead to referral to additional services are ethically suspect, unless full disclosure is provided at the time of the initial screening.

Cost, Regulations and Reimbursement

Health care advertising is a relatively costly means of communication and may be less effective in achieving the goals of a health care organization than other forms of communication. Therefore, health care facilities should approach their advertising investments with the same spirit of fiduciary responsibility that is applied to the purchase of other health care commodities, such as new equipment or buildings. Every attempt should be made to be cost-effective, to achieve measurable results, and to coordinate with other messages and public relations programs produced by the health care organization.

Health care organizations should be aware of applicable government regulations and restrictions on reimbursement for advertising expenditures.

Disclosure of Medical Record Information

Introduction

This management advisory has been prepared to assist hospitals in developing policies and procedures for the disclosure of medical record information. It addresses both internal and external disclosures as well as the patients' access to their records. While this management advisory indicates the situations in which medical record information may or may not be released, it should not be considered all-inclusive, and state/local laws should be consulted when developing any policies and procedures for medical record information release.

Medical records are maintained for the benefit of the patient, the physician, and the hospital, and are the property of the hospital. However, the content of the record is the property of the patient, and patients have the right to expect the hospital to treat their records as confidential. It is the hospital's responsibility to establish and implement security measures that safeguard both the medical record and its informational content, whether in hard copy, on film, or in computerized form, against loss, defacement, tampering, unauthorized disclosure, and use by unauthorized persons. Additionally, any individual who uses or receives information from the medical record shares in this responsibility.

The hospital should develop policies and procedures for the

preservation, retention, retirement, and release and use of medical records, including those maintained in various departments of the hospital.

Responsibility for disclosure of medical record information by the hospital should be centralized in and delegated to the Medical Record Department. The Medical Record Department, because of its expertise in medical record and release-of-information requirements, understands the characteristics of the medical record and recognizes the special situations that may require the advice of the attending physician or the hospital attorney. Except when laws or regulations dictate otherwise, the chief executive officer is responsible for the final decisions on what and under which circumstances medical record disclosures can be made.

Internal Use and Disclosure

All hospital officers, employees, and medical staff members should be made aware of the policies and procedures pertaining to the release and use of medical record information, their responsibility in maintaining its confidentiality, and the disciplinary actions that may be taken for unauthorized use or disclosure of patient information.

Access to the medical record by hospital and medical staff personnel can usually be made without

the patient's authorization. However, staff access to the medical record without the written consent of the patient depends on:

- The authority, responsibility, training, and qualifications of the hospital or medical staff member or duly appointed committee or panel requesting access
- The reason for the request
- The type of information requested

In general, staff access should be provided only on a need-to-know basis in the delivery of patient care and the management of hospital affairs, including that necessary for performing internal administrative tasks, conducting quality and utilization management programs, receiving legal counsel, planning health services, and participating in hospital-approved accreditation, certification, or licensure programs.

Even though the hospital can use medical record information for internal quality and utilization management programs without the express authorization of the individual patient to whom it pertains, all individual patient identification should be excluded from minutes and any routine reports of such findings and recommendations. When circumstances dictate otherwise, a coded method of identification may be appropriate for internal use.

This advisory, which was revised and approved by the Institutional Practices Committee in 1990, was previously known as *Guidelines on Institutional Policies for Disclosure of Medical Record Information*.

© 1990 by the American Hospital Association, 540 North Lake Shore Drive, Chicago, Illinois 60611. Printed in the U.S.A. All rights reserved.



Automatically, the hospital should:

- Establish guidelines for the use of medical records in hospital-approved education programs for physicians and other health care professionals
- Define the extent to which physicians and other health care professionals in good standing are permitted to use the medical records for bona fide study and research and define the circumstances that require patient authorization for such use

When the medical record or portions thereof are computerized, security measures should be established that restrict access to authorized individuals only along with standards that ensure the accuracy and the integrity of the information.

External Use and Disclosure

No hospital should disclose, or be required to disclose, medical record information to a third party without the patient's written authorization, unless such disclosure is:

- Pursuant to law or statutory regulation requiring the hospital to report certain information
- Pursuant to a subpoena or court order
- In response to compelling circumstances affecting a person's immediate health or safety
- Permitted by the hospital under certain circumstances in the conduct of biomedical, epidemiologic, or health services research projects
- Necessary to comply with the requirements of hospital accreditation, state licensure surveys, or certification for participation in government programs, provided

it: reports of such reviews do not directly identify individual patients

- Pursuant to the provisions of state vital statistics laws, that mandate registration of births, deaths, and fetal deaths and of other public health laws that compel reporting of certain epidemiologic conditions
- Needed in connection with the direct referral or transfer of the patient to another health care provider
- Limited to name, date of admission, and general condition, except in those instances when patients or their authorized representatives request that even this limited information not be released or when laws or regulations (for example, alcohol and drug abuse treatment) forbid the disclosure of this information

Caution should be exercised when releasing information without the patient's authorization to ensure that the individual or organization requesting the information has a valid reason to know.

Medical records should not be removed from the hospital, except upon receipt of a court order or subpoena duces tecum. In most cases, when a subpoena or court order for records is received, the court will usually accept a certified copy of the record in lieu of the original.

Even though copies of medical records that are received from other health care providers are considered a part of the patient's medical record, they should not be released when responding to requests for information.

When establishing policies and procedures for the disclosure of medical record information in response to requests from outside the hospi-

tal, the hospital should address the following:

- Nature of the requests
- Types of information requested
- Persons, agencies, or organizations who usually request information
- Situations in which a written authorization from the patient is or is not required
- Components of a valid authorization
- Requirements for the release of patient information pertaining to mental health, drug and alcohol abuse, and HIV infections
- Ensuring that patients infected with the HIV virus or being treated for mental health conditions or drug and alcohol abuse are aware of the diagnosis and that the diagnosis must be submitted on the claims for hospitalization benefits
- Conformance to laws, regulations, and other measures in the public interest
- Response to telephone requests for information as well as the call-back procedures required to verify the identity of the requester and the validity of the request
- Situations in which the attending physician should be notified of a request for information (e.g., patient access, legal requests)
- Identification and handling of special requests for information
- Establishment of reasonable charges for furnishing copies or the actual record for review

The hospital should not disclose information from the patient's medical record to the following organizations/individuals without the patient's written authorization:

- Other health care providers, unless compelling circumstances warrant immediate disclosure
- Third-party contractors, unless the disclosure is made in accordance with provisions of a particular hospital/third-party or patient/ third-party contract for inspection of certain portions of the medical record for claims processing, financial audit, utilization review, or case management
- Attorneys, tribunals, members of the court, or government investigation and law enforcement agencies, unless disclosure is compelled by judicial subpoena, court order, properly issued and authorized administrative summons, or as otherwise mandated by law
- Administrative personnel, teachers, or nurses in the local school system
- Employers, unless such disclosure is pursuant to any state or local statute(s) providing specific authority for such disclosure

Additionally, the hospital's chief executive officer should determine whether or not to permit medical records maintained by the hospital to be used by a third party for conducting biomedical, epidemiologic, health services, or related research and whether or not the patient's authorization is required in accordance with established hospital policy. This decision should be based on whether:

- The importance of the project's purpose outweighs any nominal risk to individual privacy rights
- The proposed methodology violates any limitation under which the medical record information was collected
- The safeguards are adequate to protect the confidentiality and

integrity of the medical record and information therein

- The further use or redisclosure of any medical record information in patient-identifiable, physician-identifiable, or hospital-identifiable form requires the written consent of the chief executive officer of the hospital, who shall exercise due regard for the rights of others affected
- The medical records of the hospital are a suitable source of information for the purpose for which they are to be used
- The third party makes appropriate commitments for safeguarding the patient's privacy, including, in some instances, an agreement to refrain from contacting the patient or others

Responses to all written requests pertaining to notification or access should be made promptly, if possible, within 10 business days following their receipt. If a full response cannot be made within that time, an acknowledgement should be sent to indicate that a response will be forthcoming.

Caution should be exercised when releasing information from the medical records of patients who have been treated for alcohol, drug abuse, mental health conditions, and HIV infections. Although federal regulations specifically address the release of information from alcohol or drug abuse patient records, no such federal regulations exist for the treatment of mental health conditions or HIV infections.

However, most states have laws protecting the confidentiality of mental health records and they should be consulted when establishing any policies and procedures. The American Medical Record Association's guidelines for

release of information from the records of patients infected with the HIV virus specify that information should be released only with the patient's informed written consent. The guidelines for this consent form are as outlined in the section on Authorization for Disclosure.

In response to any request for information, the hospital should disclose only the information that is stated on the authorization. Hospitals should not honor any authorizations that specify "any and all information" or other such broadly inclusive statements. Requesters should be made aware of their responsibility not to further disclose such information, make copies of it, or use it for a purpose not specified in the authorization, unless further disclosure is expressly permitted in the original authorization or is by necessary implication inherent in the purposes of the original consent or authorization.

Audio or video tapes may or may not be considered a part of the medical record, depending on the purpose for which they were made. Hospitals should establish a policy that specifies the instances in which audio or video tapes are considered a part of the medical record.

When an individual or organization requests a copy of any video or audio tape, the hospital should verify that the release is consistent with hospital policy and/or state statutes. If the decision is made to release the tape, a duplicate tape should be made and forwarded to the requester and the original should remain within the facility.

When a claim against the hospital or its medical staff members is threatened or pending, or after such has actually been filed, requests by

patients or their attorneys or other representatives for access to the patient's medical records should be brought to the hospital attorney's attention immediately. The attorney may then advise whether, when, how, and under what circumstances such access should be granted or copies furnished to the requesters.

The hospital should maintain either the original or a copy of the patient's disclosure authorization, which should be made available for examination by the patient. In addition, a notation/log should be kept of all disclosures to third parties. At a minimum, this log should contain the patient's name and medical record number, the name of the individual/organization to whom the information was released, the information released, the date of the release, and whether any payment was received for the information furnished.

Patient Disclosure

The American Hospital Association's *A Patient's Bill of Rights* states: "The patient has the right to obtain from his physician complete current information concerning his diagnosis, treatment, and prognosis in terms the patient can be reasonably expected to understand. When it is not medically advisable to give such information to the patient, the information should be made available to an appropriate person in his behalf."

The laws (statutory or judicial) of most states recognize a reasonable right of access to medical record information by the patient or nominees. The patient's right of access in no way abrogates the hospital's property rights to the record and its right to establish

reasonable procedures for access to the patient's record.

The attending physician should be notified of the patient's request for access to the medical record.

Records containing information that might be detrimental to the physical and/or mental health of the patient, as determined by the attending physician, should be released in a form that minimizes any adverse effect on the patient.

When it is known that patient access to medical record information may be medically contraindicated, the hospital may require that a physician or designee inspect the record and communicate the appropriate information.

Additionally, a patient has the right to:

- Verify that the hospital has created and is maintaining a medical record pertaining to care or services provided to the person by the hospital
- Determine if a disclosure of the medical record has been made and to whom
- Review the medical record, unless access is believed by the attending physician to be medically contraindicated
- Request a copy, upon payment of reasonable charges for the service, and may request correction or amendment of information
- Designate a personal representative(s) or duly authorized nominee(s) to have reasonable access to information within the medical record

Policies and procedures for patient access to medical records should include:

- Measures to provide evidence of all disclosures of medical record information, other than those

made during routine use within the hospital, and the retention of such evidence with the record from which the information was disclosed

- Notification of the attending physician when a patient requests access to the medical record
- Designation of a committee or a hospital staff member and a medical staff member who are granted authority and responsibility for implementing and overseeing hospital policy and procedures on patient access to medical records and reviewing judgments thereunder
- Steps involved in receiving and considering patient requests for correction(s) or amendment(s) to their medical records, including notification to the attending physician and notification to the patient as to the acceptance or denial of the request. These requests should be submitted in writing and should specify the entry or entries in dispute. With the exception of requests for correction of such items as time of admission, birthdate, spelling of last name, and other such admission data that can be handled by qualified employees, the attending or other responsible physician(s) should be notified of requests for corrections or amendments. The hospital and attending physician(s) will decide whether or not the correction or amendment is to be made
- Establishment of a mechanism, which might consist of a committee or panel, to review denial(s) of patient request(s) to correct or amend their records
- Establishment of special procedures to handle requests by the patient or the patient's family for access to medical records when

direct access apparently could be harmful to the patient

- Identification of the rights of minors to access to the medical record as may be permitted under general state law or state law permitting minors to seek on their own behalf, without the knowledge or consent of their parents, treatment for certain conditions, such as venereal disease, alcohol or drug abuse, pregnancy, and for family planning and abortion services
- Presence of a designated hospital employee at all times to ensure the integrity of the review. To the extent feasible or desirable, a physician or qualified employee may be present to assist the patient in reading the entries in the record

If a decision is made to correct or amend the medical record, the patient should be so advised. Any correction or amendment should not obliterate the material corrected.

If the request for correction or amendment is not granted, the patient should be informed that a statement of the patient's disagreement can be filed with the hospital and that the disputed entries in the medical record will be appropriately annotated to reflect this disagreement. Any further disclosure of the medical record will include this statement of disagreement and the annotations.

Authorization for Disclosure

In keeping with the principles for informed consent, a valid authorization for disclosure of patient information should:

- Be dated after treatment was instituted and no more than 90

days prior to the date on which information is requested

- Contain the name of the individual or organization to whom the information is to be released
- Be addressed to the facility from which the information is requested
- Include the patient's full name, address, date of birth, and the purpose for the release
- Be specific as to information to be released, including dates of treatment and any restrictions by the patient for disclosure of a specific medical condition, injury, time period, and/or any other type of specified information. Authorizations that specify "any and all information" should not be honored
- Include a statement that the authorization is subject to revocation at any time to the extent that action has been taken in reliance thereon, and a specification of the date, event, or condition upon which it will expire without express revocation
- Be signed by the patient or legal guardian

A special authorization for the disclosure of information from drug or alcohol abuse patient records is required. In addition to the items described above, a valid authorization for release of information from the records of drug/alcohol abuse treatment patients should include a prohibition on redisclosure.

Additionally, when disclosure is made from drug or alcohol abuse patient records, it must be accompanied by the following statement: "This information has been disclosed to you from records whose confidentiality is protected by federal law. Federal regulations prohibit you from making any fur-

ther redisclosure of it without the specific written consent of the person to whom it pertains or as otherwise permitted by such regulations. A general authorization for the release of medical or other information is not sufficient for this purpose."

Upon admission to the hospital, the patient can be requested to sign an authorization for release of information. This "prior to treatment" authorization should be used only for:

- Verifying a patient's benefits
- Including diagnostic/procedural information on the UB-82
- Providing information to insurance companies or utilization review organizations for continued stay review or case management

This "prior to treatment" authorization is *not* sufficient to permit additional release of information after discharge from the hospital.

General Guide for the Release of Patient Information by the Hospital

Adapted from "Release of Information" in *Hospitals and the News Media: A Guide to Good Media Relations* by Mary Laing Babich, copyright 1985 by American Hospital Publishing, Inc. (out of print). For more information, consult *Public Relations in Health Care. A Guide for Professionals* by Kathleen Larey Lewton, copyright 1991 by AHPI. To order the book or additional copies of this booklet, call AHA's Department of Order Processing at 800/AHA-2626.

**American Society for Health Care
Marketing and Public Relations**
of the American Hospital Association



Condition of Patient

Nature of accident or injury

**Matters of Public Record
Coroner's Cases**

Accidents and Police Investigations

Information in this booklet is provided only as a guideline for hospitals when dealing with the news media. It is important to be aware that laws regarding patient privacy, confidentiality, and "public record cases" vary from state to state. The PR manager should consult with the organization's legal counsel before finalizing any policies on release of patient information.

The following information may be released by the hospital for any inpatient or emergency department patient

Name Address Occupation Sex Age Marital status

However, the restrictions described should be observed whenever possible or practical before any information is released

Condition of Patient

Except for the following one-word conditions, no information about the patient may be released without the patient's permission. Only a physician may discuss the patient's diagnosis and/or prognosis, if the patient has given permission for the physician to do so. The following terms can be used to describe the patient's condition:

Good. Vital signs are stable and within normal limits. Patient is conscious and comfortable. Indicators are excellent.

Fair. Vital signs are stable and within normal limits. Patient is conscious but may be uncomfortable. Indicators are favorable.

continued

Condition of Patient

Nature of accident or injury

Matters of Public Record Coroner's Cases

Accidents and Police Investigations

Condition of Patient *continued*

Serious. Vital signs may be unstable and not within normal limits. Patient is acutely ill. Indicators are questionable.

Critical. Vital signs are unstable and not within normal limits. Patient may be unconscious. Indicators are unfavorable.

Unconscious. The hospital may release information that the patient was unconscious when brought to the hospital.

Dead. The death of a patient is presumed to be a matter of public record and may be reported by the hospital after the next of kin has been notified or after a reasonable time has passed. Information regarding the cause of death must come from the patient's physician, and its release must be approved by a member of the immediate family (when available).

Nature of accident or injury

The hospital spokesman may give out only limited information about the various kinds of accidents or injuries in order to protect the privacy of the patient.

Battered children. The spokesman may not discuss possible child abuse. However, the injuries sustained by the child may be described as indicated below.

Burns. The spokesman may state that the patient is burned, but the severity and degree of burns may be released only after a physician's diagnosis.

Fractures. The spokesman may provide information on the location of the fracture only if a limb is involved and may say whether the fracture is simple or compound.

Head injuries. The spokesman may state that the injuries are of the head. It may not be stated that the skull is fractured until diagnosed by a physician.

Internal injuries. The spokesman may state that there are internal injuries, but no information may be given as to the location of the injuries until a physician has made a diagnosis.

Intoxication or drug abuse. The spokesman may not provide information that the patient was intoxicated or had abused drugs or characterize the patient as an abuser. The spokesman should be wary of indicating a diagnosis that might imply substance abuse; for example, saying that a patient had cirrhosis could indicate alcohol abuse.

continued

Nature of accident or injury**Matters of Public Record
Coroner's Cases****Accidents and Police Investigations**

Nature of accident or injury continued

Poisoning. The spokesman may state only that the patient is being treated for suspected poisoning. No statement may be made concerning either motivation or circumstances surrounding a patient's poisoning. The suspected poisonous compound may be identified only by the patient's physician.

Sexual assault. The spokesman may not say that the patient has been sexually assaulted nor provide information regarding the nature of the sexual assault or injuries. Only the condition of the patient may be given.

Sexually transmitted and communicable diseases. The spokesman may not provide information that the patient has a sexually transmitted or communicable disease. The spokesman should be careful not to indicate a diagnosis that might imply a communicable disease. For example, saying that a patient has Kaposi's sarcoma could indicate the patient has AIDS.

Shooting or stabbing. The spokesman may provide the number of wounds and their location if these facts have been definitely determined by a physician. No statement may be made as to how the shooting or stabbing occurred.

Suicide or attempted suicide. The spokesman may not provide any statement that there was a suicide or attempted suicide.

Transplant recipients and organ donors. The spokesman may release information regarding the nature of the transplant and the condition, age, and sex of the recipient. However, the release of the names of the recipient and/or donor requires prior consent. If the donor is deceased, the name may not be given out without the consent of the legal next of kin.

Matters of public record

Matters of public record refer to those situations that are by law reportable to public authorities, such as the police, coroner, or public health officer. Examples of matters of public record are the following:

Persons under arrest or held under police surveillance

Persons brought to the hospital by the fire department or by any law enforcement agency

Persons who have been shot, stabbed, poisoned, injured in automobile accidents, or bitten by dogs or other animals

Persons with any other injuries that are usually reported to governmental agencies regardless of the mode of transportation to the hospital.

Coroner's Cases

Generally, in accordance with state law, the hospital must provide the coroner with information in any of the following circumstances:

When the body is unidentified or unclaimed

When a sudden death is not caused by a readily recognized disease or when the cause of death cannot be properly certified by a physician on the basis of prior (recent) medical attendance

continued

**Matters of Public Record
Coroner's Cases**

Accidents and Police Investigations

Coroner's Cases continued

When the death occurred under suspicious circumstances, including those deaths in which alcohol, drugs, or other toxic substance may have a direct bearing on the outcome

When the death occurred as a result of violence or trauma, whether apparently homicidal, suicidal, or accidental (including those resulting from mechanical, thermal, chemical, electrical, or radiational injuries or from drownings or cave-ins) and regardless of the time elapsed between the time of injury and the time of death

When there is a fetal death, stillbirth, or death of any baby within 24 hours after its birth and the mother has not been under the care of a physician

When the death has resulted from an abortion, whether therapeutic or criminal, self-induced, or otherwise

When operative and peri-operative deaths are not readily explainable on the basis of prior disease

The hospital should check with its attorney to find out what other types of situations are required by state law to be reported to the coroner.

Accidents and Police Investigations

The spokesman may release the name, address, age, nature of injury, condition (if determined), and the disposition of such patients, that is, whether they have been hospitalized. No attempt should be made to describe the event that caused the injury, and no statement about any of the following should be made:

Whether a person was intoxicated

Whether the injuries were the result of an assault, attempted suicide, or accident

Whether a patient was poisoned (accidentally or deliberately)

Whether a patient is suspected of being a drug addict

The circumstances that resulted in a patient's being shot or stabbed

The circumstances related to an automobile or industrial accident

APPENDIX 2.—STATEMENTS SUBMITTED FOR THE RECORD

NATIONAL RESEARCH COUNCIL

COMMISSION ON BEHAVIORAL AND SOCIAL SCIENCES AND EDUCATION

2101 Constitution Avenue Washington, D.C. 20418

COMMITTEE ON NATIONAL STATISTICS

Telephone 202-334-3096

28 March 1994

The Honorable Gary A. Condit
Chair, Subcommittee on Information, Justice,
Transportation and Agriculture
U.S. House of Representatives
1123 Longworth House Office Building
Washington, DC 20515-0518

Dear Congressman Condit:

The Committee on National Statistics is concerned about the provisions for privacy and confidentiality of health care information in legislation being considered by the Congress. I write to bring to your attention some issues we believe should be addressed in the legislation.

Many proposals for health care reform call for the development of a national information system that will contain, for virtually all Americans, health care information in electronic form and in a uniform format. By *health care information*, we mean records about individual participants. These records include enrollment data, such as name, address and other identifiers; basic demographic data, such as age and race; and encounter or claims records with limited information about health care, such as diagnosis, provider, services, results, and charges.

Responsible and carefully protected access to health care information for research and other statistical uses can benefit society greatly by providing key information about the health care system and by informing other national policies. By *research and statistical uses* of data, we include description, evaluation, analysis, inference, and research, the results of which are not concerned about specific individuals. These uses are distinguished from regulatory, administrative, or enforcement uses, which do affect specific individuals. With proper safeguards for privacy and confidentiality, research and statistical uses of health care information will not harm individuals.

The Committee has two concerns. The first and foremost is that privacy and confidentiality of health care information be adequately protected. The second is that the U.S. health care system, individual health care subscribers, and the public as a whole benefit from access to that information for research and other statistical purposes in ways that protect confidentiality. It is not necessary to sacrifice either confidentiality or the benefits of information: both are possible if legislation provides for responsible access and demonstrated, effective means to protect confidentiality.

The Honorable Gary A. Condit
 28 March 1994
 Page 2

Any health care legislation should provide for protecting privacy and confidentiality of health care information and for achieving the many benefits of important research and statistical uses of the information, including benefits not directly related to the health care system. Legislation can achieve these goals by

- prohibiting data about an individual that are collected or maintained for research and other statistical uses from being used in any administrative or enforcement action affecting that individual;
- extending confidentiality protection to identifiable data about individuals, wherever the data are maintained;
- providing sanctions against unauthorized disclosures by any user;
- authorizing access to health care data about individuals for research and statistical purposes whenever confidentiality can be assured; and
- creating an independent federal advisory body charged with fostering a climate of enhanced protection for all federal data about persons *and* responsible data dissemination for research and statistical purposes.

Although information on health care may be more sensitive than other types of information, many issues of confidentiality and of research and statistical uses of administrative records are not unique to health care information. Since its establishment in 1972, the Committee and some of its panels have addressed these issues in several different contexts. A panel of the Committee and of the Social Science Research Council recently completed a major study on privacy and confidentiality: *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics* (National Academy Press, 1993); a reprint of the "Executive Summary and Recommendations" is enclosed. The report describes many effective practices, both administrative and technical, by which federal statistical agencies protect confidentiality of information on individuals while allowing access to the information for important research and statistical purposes.

Another panel of the Committee considered possible uses of provider health records as part of ongoing health care surveys in its report, *Toward a National Health Care Survey: A Data System for the 21st Century* (National Academy Press, 1992). The Committee's concerns are based on the findings of these panel reports and on its own assessment of confidentiality issues pertinent to health care information. We have also considered a recent report of the Institute of Medicine, *Health Data in the Information Age: Use, Disclosure, and Privacy* (National Academy Press, 1994).

The Honorable Gary A. Condit
28 March 1994
Page 3

Protecting privacy and confidentiality

It is a basic responsibility of any federal statistical agency to protect the confidentiality of individually identifiable data, whether the data are collected directly, as in voluntary surveys, or obtained from administrative records. By *individually identifiable data*, we mean data from which the identity of an individual can be determined, either because the data include identifiers (such as name or Social Security number) or because the data include information in sufficient detail to infer the identity. By *administrative records*, we mean the records of an administrative program, such as Social Security.

We believe that the most effective way to protect the confidentiality of health care information that is provided for research and statistical purposes is to enact legislation to codify the principle of *functional separation* enunciated by the Privacy Protection Study Commission in 1977. This principle states that data on an individual, when collected for research or statistical purposes, should not be made available for any enforcement, compliance, or administrative action affecting the individual. The commission noted the benefits of research and statistical uses of data to society as a whole and the rich lode of administrative data in the federal government that had barely been tapped for research and statistical purposes. The commission recommended (p. 574):

that the Congress provide by statute that no record or information contained therein collected or maintained for a research or statistical purpose under Federal authority or with Federal funds may be used in individually identifiable form to make any decision or take any action directly affecting the individual to whom the record pertains, except within the context of the research plan or protocol, or with the specific authorization of such individual. (*Personal Privacy in an Information Society*, U.S. Government Printing Office, 1977)

The same principle should apply to data collected for an administrative program and transferred to another agency or organization for research or statistical purposes. One of the key recommendations of the Committee's Panel on Confidentiality and Data Access was that statistical records across all federal agencies be governed by the principle of functional separation (see Recommendation 5.1 in the panel report).

Benefits of health care information

Health care information is needed for individual treatment and the management of the health care system. Physicians need immediate access to that information and the results of research on that information in order to make accurate diagnoses and recommend appropriate treatment. But the information is also needed for effective monitoring of the trends that

The Honorable Gary A. Condit
28 March 1994
Page 4

affect the costs of health care and for planning for the changes in health care needs of Americans. What are the trends in the incidence of disability and the use of long-term care facilities, and what are their budgetary implications? Are the goals of universal coverage and equal access to plans by all persons being met? Information is needed for research to answer these questions and also for a better understanding of social factors related to health and health care coverage: occupational exposures to toxic chemicals; the prevalence of mental disorders and other chronic conditions; the relationship between health status, health care coverage, and decisions on retirement; and, more generally, the social, economic, and demographic characteristics of the U.S. population. Research on such important topics has long been done without harming patients.

States and the federal government are increasingly being held accountable for developing information needed to monitor the health care system and to ensure its effectiveness, efficiency, and fairness to all participants. Their ability to meet the information needs for these purposes and to realize many other important benefits of health care data will be lost if legislation fails to provide for responsible access to health care data for research and statistical purposes. By responsible access, we mean access in ways that protect confidentiality.

Data from administrative records, such as Medicare records, may provide information on health and other outcomes, but it is often not possible to understand what may have caused the outcomes unless the data can be combined with other data, such as those from surveys that collect information on disabilities, for example. Thus, research will frequently require access to individually identifiable records as an intermediate step in collecting or compiling data for analysis. The results of such research, however, do not identify specific individuals. Legislation should fully protect the confidentiality of individually identifiable health care information while making possible the necessary data linkages for research to inform health care and other public policies.

We note, in particular, that it is a well-established and productive practice of statistical agencies to release public-use data files, which have been prepared by stripping individual identifiers (such as name and Social Security number) and taking other precautions to ensure that there is virtually no possibility of identifying individuals. No legal barriers or restrictions should be placed on the release of similar public-use files based on data from the new health information system.

Although very useful, however, public-use files do not satisfy all important needs for research on issues of public policy. Different research investigations or policy studies may require different data to be combined or data to be combined in different ways. Moreover, data from public-use tapes, because they are anonymous, cannot be combined with further data that may be needed, such as information from Social Security earnings records.

The Honorable Gary A. Condit
28 March 1994
Page 5

Just as health care policies affect and are affected by other public policies, the health care information system will contribute to and be served by other information in the federal statistical system. With safeguards for confidentiality, the nation benefits today from statistical uses of information from administrative records. For example, population estimates are improved through information from tax records and from birth and death certificates. Understanding of disability and of long-term care has been improved because a national survey obtains, with the permission of respondents, accurate information from their health care providers. The understanding of decisions on retirement and on health care in retirement has been improved because another national survey obtains information on earnings from Social Security records and on health care from Medicare records.

Serious attention is now being given to how to conduct an improved decennial census at lower cost through greater use of administrative records. Basic health care enrollment information could be used to improve the frames, or lists, for drawing national samples or for taking a census without the current costly operations. The demographic information from health care enrollment records could also be used to improve population estimates between censuses. Such uses would require Census Bureau access to identifiable records, but not to sensitive health information.

The U.S. health care information system, with appropriate confidentiality safeguards, should be designed to serve important research and statistical purposes. In addition, data should be collected with appropriate concern for the ethical treatment of those to whom the data pertain. The report of the Panel on Confidentiality and Data Access recommends, for example, that certain kinds of basic information be given to all people asked to provide data in censuses and surveys (see Recommendation 3.2). It is important that both respondents to surveys and those who complete administrative forms be informed about planned or expected uses of their data and the possibility of unanticipated future uses for research or statistical purposes.

Realistic laws for confidentiality

Some bills before Congress suggest that the confidentiality of individual health records can be protected by stipulating that data collected for one purpose shall not be used for any other purpose. Such a blanket prohibition would be very harmful to society by denying it the benefits of legitimate research and statistical uses of the data. No one can foresee all potential uses of data that would benefit society. If such prohibitions were enacted and enforced, society would lack important information that it could obtain only at greater cost through new data collection activities that might intrude further on individual privacy.

The Honorable Gary A. Condit

28 March 1994

Page 6

We suggest, instead, that legislation authorize access to individually identifiable health care data for research and statistical purposes in circumstances in which confidentiality can be assured. Confidentiality protection should extend to the data wherever they are maintained. Legal sanctions should protect against unauthorized disclosures by all researchers and other data users, whether they are inside or outside the federal government (see Recommendation 5.3 in the report of the Panel on Confidentiality and Data Access). These same suggestions should apply equally to all confidential data collected for the government.

The Institute of Medicine report (noted above) focuses on information to improve the health of individuals and the performance of the health care system. The Committee on National Statistics, however, is also concerned with uses of the information for other important research and statistical purposes, especially by the federal statistical agencies. In this broader purview, we believe that access to individually identifiable health care information for these purposes should be allowed in ways that protect confidentiality. In particular, respondents to voluntary surveys should be able, with informed consent, to permit selective access to their health care information (see Recommendation 3.3 in the report of the Panel on Confidentiality and Data Access).

Agencies can further protect the confidentiality of data they provide for research and statistical purposes. The report of the Panel on Confidentiality and Data Access describes additional procedures for doing so. These procedures include statistical techniques for reducing the risk of unintended disclosure and administrative arrangements, such as licenses that regulate the conditions for access to and use of data. Yet it must be recognized that every procedure carries a risk, albeit a very low one, of an inadvertent disclosure. Requiring zero risk for such disclosures is an unrealistic and unachievable standard (see Recommendation 5.2 in the panel report). Legislation should result in regulations and policies that establish standards of reasonable protection to safeguard the identity of individual respondents and appropriate sanctions for violations.

A federal advisory body

We do not favor the establishment of a commission or other group with the authority to rule on each request for access to health care information for research and statistical purposes. These decisions are better made by agencies or organizations that either collect or manage the data, with appropriate guidance. Therefore, we support the concept of an independent federal advisory body charged with fostering a climate of enhanced protection for all federal data about individuals *and* responsible data availability for research and statistical purposes (see Recommendation 8.5 in the panel report). The advisory body could provide clear guidance for federal agencies, institutional review boards, and researchers on appropriate and responsible data access, and it could advise Congress on the effects of

The Honorable Gary A. Condit

28 March 1994

Page 7

legislation. The advisory body could address important questions that pertain to statistical uses of information from records of administrative programs. For example, what control should individuals have over such data? What should they be told about statistical uses? Under what circumstances should informed consent or notification be required? Should administrative records be used to identify individuals with specific health conditions to be contacted for a research purpose?

The advisory body could also serve to communicate to the public how confidentiality is protected while allowing for the legitimate and beneficial research and statistical uses of their information. What is most important, in our view, is that an advisory body reflect in its name, composition, and staff, as well as in its charge, two purposes: protecting the confidentiality of health care information and fostering responsible access to that information for research and statistical purposes.

We are pleased that you are working toward the passage of legislation on this very important issue. The Committee on National Statistics stands ready to help you in any way it can.

Sincerely,



Norman M. Bradburn, *Chair*
Committee on National Statistics

Enclosures

Membership, Committee on National Statistics
Description of the Committee
Executive Summary and Recommendations,
Private Lives and Public Policies



May 12, 1994

Hon. Gary Condit
 Chairman
 House Government Operations Subcommittee on Information,
 Justice, Transportation, and Agriculture
 B-349C RHOB
 Washington, DC 20515

Dear Mr. Chairman:

The Information Technology Association of America (ITAA) submits these comments for the record of the hearings on H.R.4077, the Fair Health Information Practices Act of 1994. ITAA, together with its 21 regional affiliated technology councils, represents 3,000 companies offering computer software and services, and systems integration.

ITAA supports creation of a national statutory right of privacy in health care records. We welcome the opportunity to redress lack of uniform, reliable national protection as part of overall health care reform. ITAA is pleased that your bill steers away from certain ill-considered proposals, finds the bill generally acceptable, but has several concerns.

Scope of Coverage

ITAA's first principle is that the scope of newly-created protection must be complete

- * to assure full protection of the inalienable personal interest of privacy
- * to gain citizen confidence
- * to enable nationwide design and engineering of the advanced information systems that will improve care and drive down costs.

That implies, first, that Congress must assure that records created under private supplemental insurance are equally protected as under any federally-supervised plan. It implies, second, rejection of the proposal of the Workgroup on Electronic Data Interchange (WEDI) to extend national statutory coverage only to electronic, and not paper-based, records (as indicated in the April 27 testimony of Mr. Joel Gimpel for WEDI, p. 3). This illogical proposal would elevate form over substance. If incentives are needed to promote

Information Technology Association of America

modernization, they must be other than ones undermining public confidence and undercutting the fair and logical scope of privacy protection. ITAA congratulates you for having made this fundamental choice correctly in Section 3(a)(3).

Rights and Duties of the Parties

In a complex multiparty context, the appropriate rights and duties should fall to the appropriate parties. Generally speaking, there are three classes of participants in the health-care system: individual patients, direct caregivers, and third-party service vendors. Caregivers maintain the patient relationship and decide what data to collect.

Caregivers thus bear the primary duty of care for records, their accuracy, and nondisclosure. When they entrust those records to others for processing, the third parties are bound primarily by contract, but also by ordinary tort-law standards of due care. Patients should have redress against the caregiver for wrongful disclosures, or at most against individuals employed by third-party outsourcers acting contrary to correct company policy and procedure. Patients' right of access to files about them is properly directed to direct caregivers. By the same token, the bill evidently aims to achieve expedited transfer of records among the parties providing treatment and payment without the necessity for patient consent in each instance.

ITAA appreciates that this understanding seems to be reflected in the bill. In this regard, however, ITAA questions the meaning of Sections 121(b) -- for expedited records transfer in the limited cases -- and 122(b) -- generally, for individual consent otherwise. It is not completely clear to us that the purpose of having data processing or transmission service performed pursuant to a written service contract between the trustee and the service provider qualifies as a "purpose that is authorized under this Act" in Section 121(b). If a change in the statutory language seems undesirable, this point should at least be clarified in the legislative history.

Government Access to Health Records

ITAA's second principle is that, consistent with the Fourth Amendment and Electronic Communications Privacy Act, government access to health care records must be by proper legal process, whether by subpoena or court order. ITAA is therefore disturbed by the certification process provided for in Section 129 that allows for law enforcement access without court process. No records are more sensitive to the individual citizen than law enforcement records. Even if the records so obtained will not be used against the citizen, and even if the party producing the records will be held harmless against claims by the individual (Section 161(h)), this is simply not the right policy.

ITAA fails to understand why law enforcement authorities cannot make an adequate showing before a judge that records must be obtained so as to combat fraud, for example. Especially disturbing is the possibility that enactment of this provision, as a national standard, in some cases could actually decrease the individual's level of protection compared to what it is today in jurisdictions where court process is required. ITAA therefore calls for deletion of the certification bypass of court process as an unwarranted abridgement of personal rights at odds with the bill's stated findings.

Related to the legal standards for law enforcement access is the Administration's widely-criticized and ill-conceived initiative to promote the clipper/capstone chip and tessera card. Congress needs to legislate against the background of this National Security Agency initiative that regrettably has become Administration policy. The National Institute of Standards and Technology (NIST) has adopted the clipper chip as a Federal Information Processing Standard (FIPS) over perhaps the greatest public opposition to any federal proposal in recent years. Under the dual-key system and H.R.4077, law enforcement agencies will have the technical and legal ability get into citizens' most intimate records without their knowing it. The Administration is now apparently moving toward designation of key-holders outside the Executive Branch, a minimum condition for any meaningful escrow to exist at all. Even if this rudimentary step is taken, however, it must be assumed that law enforcement agencies will take maximum advantage of whatever the new provisions apply.

State Preemption

Section 304 provides for partial, but not complete, preemption of state laws. In ITAA's view, the bill must not stop short of full preemption if it is going to provide the foundation for the national electronic systems clearly anticipated in Findings 4 and 5. Without complete preemption, systems integrators will simply lack the confidence to go ahead and execute systems designs based on the requirements of this bill. Either vendors will be able to rely on translating this bill into practice without extensive further legal research, or they won't. As the bill stands today, the assurance the information technology industry has been hoping for and expecting has not been provided. ITAA calls for strengthening Section 304 to provide for complete preemption in accord with the logical implication of Findings 4 and 5.

Regulations and Notification

ITAA believes that a timely solution is needed to the absence of national health records privacy policy. Vendors need to start soon to design nationwide (and even international) systems to improve care and to drive down costs soon. Privacy standards become design requirements for systems integrators and database vendors.

A two-year phase-in period is excessive. The basic principles of privacy protection are well understood and are contained in the 1981 Transborder Data Flow Guidelines of the Organization for Economic Cooperation and Development (OECD). What is needed is not new principles, but prompt implementation. Vendors cannot wait until 1997 to know what the national rules are going to be. Based on enactment by the end of this Congress, the effective date should be no later than January 1, 1996.

Also, the bill should clarify whether the notification to be created by the Secretary of Health and Human Services (HHS) is mandatory or permissive (Section 145). ITAA prefers that it be permissive and sees no reason for federal law to require parties satisfied with their existing notices -- provided, of course, that they meet the bill's disclosure standards -- to go to the expense of change for its own sake.

The Payments System

ITAA believes Section 151, relating to debit and credit card transactions, to be adequate for these identified forms of payment. By the same token, the bill does not specifically address other forms or means of payment that often involve the participation of third parties in the authorization, payment, and collection process. Under managed care, pharmacies, for example, often receive only a nominal \$5 or \$10 copayment from the recipient, relying on third parties for the balance due. How would the bill address situations in which the insurer or other expected payor later refuses to pay?

In other new programs, some third parties in essence "factor" the receivables on behalf of the provider so as to allow for more prompt payment, in exchange for a discount-based fee to the factoring agent. Is this acceptable? How would the factoring agent be able to receive adequate information about the recipient to collect unpaid balances? Such questions lead ITAA to conclude that Section 151 should be broadened to include any accepted type of payment process.

International Data Transfer

H.R.4077 correctly anticipates the international transfer of health care data. Nonetheless, ITAA finds the equivalency standard (Section 152(a)(2)) problematic in the absence of a binding global instrument with a set of substantive data protection standards. A provision that could be seen as an attempt to legislate unilaterally in this context might be unwise. Indeed, with regard to the draft data protection directive by the European Commission, U.S. industry was relieved -- despite other misgivings -- that the relevant standard to which other countries would be held would be "adequate" rather than "equivalent" protection.

ITAA suggests instead the borrowing the phrase "adequate and effective" from the intellectual property context, where the rights of U.S. citizens likewise can be violated abroad. As the U.S. has been vigilant in this regard, no one could believe that the U.S. were not serious about data protection, yet the phrase would not have the troublesome implications of "equivalent."

Alternate Dispute Resolution (ADR)

ITAA, having promoted ADR in other policy contexts as well as in privacy, applauds the inclusion of Section 163 in H.R.4077. ITAA suggests only that the word "develop" may have an inappropriately narrow meaning. ITAA sees no apparent difficulty in HHS's adopting or adapting ADR methods already developed elsewhere. If a wording change in this section seems undesirable for whatever reason, the legislative history should explain that HHS is not expected only to develop new procedures from scratch, but that it should seek to identify preexisting mechanisms that may be put to use, either directly or with appropriate modifications, to resolve disputes about health care data protection.

* * * * *

Mr. Chairman, ITAA appreciates your leadership in this issue lying at the intersection of health care reform and information technology policy. We would be pleased to discuss any of our comments in detail.

Yours truly,

David Peyton

David Peyton
Senior Vice President
Processing and Network Services Division

STATEMENT SUBMITTED FOR THE RECORD

OF THE U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT OPERATIONS

SUBCOMMITTEE ON INFORMATION, JUSTICE,
TRANSPORTATION AND AGRICULTURE

REGARDING
THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1994
H.R. 4077

BY

SMART CORPORATION
2201 AMAPOLA COURT
TORRANCE, CALIFORNIA 90501

MAY 17, 1994

I. Introduction

Smart Corporation appreciates this opportunity to comment on the Fair Health Information Practices Act of 1994 (H.R. 4077). Smart commends Chairman Condit as well as the other Members and the Staff of the U.S. House of Representatives Committee on Government Operations Subcommittee on Information, Justice, Transportation and Agriculture for their efforts to ensure that the privacy of individually identifiable health information is protected. H.R. 4077 constitutes a significant step in meeting this important objective, particularly as the Nation scrutinizes the structure and operation of the health care industry.

Smart Corporation is the founder and leader of the medical records copying industry. Smart contracts with hospitals and other health care providers to photocopy medical records for such authorized users of health information as patients, insurance companies, attorneys, health care providers and government agencies, among others. Since its inception in 1976, Smart's client base has increased significantly. Today, the company serves more than 2,600 health care providers in 44 states and employs approximately 2,200 people.

The primary reason Smart has experienced such significant growth is that it can provide photocopies of medical records in a more cost-effective and timely manner than can health care providers who copy records in-house. Approximately 65 percent of the Nation's hospitals use a medical record copy service because of the tremendous cost savings they realize by eliminating the labor, equipment and supplies needed to respond to medical record requests.

However, an equally, if not more important function Smart Corporation serves for private citizens and the general public (and for purposes of analyzing H.R. 4077) is to ensure the privacy of health information, and that only authorized information is released. In this regard, Smart can provide the Subcommittee with valuable insight into the health information industry and the critical role it plays in maintaining the patient's right to privacy.

II. Smart Corporation Supports H.R. 4077 Generally with a Specific Concern Noted

Smart Corporation is a member of the American Health Information Management Association (AHIMA), the organization which represents 35,000 credentialed professionals who are responsible for managing health information. AHIMA has played an instrumental role in the development of H.R. 4077 by providing model legislation for, and testifying before, the Subcommittee. AHIMA has lent its general support for H.R. 4077 with specific concerns noted in its March 4, 1994 testimony before the Subcommittee.

Smart Corporation joins AHIMA in its praise for H.R. 4077. As noted above, the bill marks a substantial step forward in creating uniformity among the states in protecting the confidentiality of health care records. However, Smart Corporation, in its capacity as an expert in the medical records copying industry, would like to address one specific concern raised by H.R. 4077.

Section 111 of H.R. 4077, subsection (d), provides that certain conditions may be imposed related to the inspection of protected health information. More specifically, the bill provides that a health information trustee may:

- "(2) **charge a reasonable fee (not greater than the actual cost) for--**
 "(A) permitting inspection of information under this section; and
 "(B) **providing a copy of protected health information under this section.**" [Emphasis added.]

Smart Corporation believes capitation of fees related to copying medical records at "actual" cost to be ill-advised. In addition, other limitations on copying charges (i.e., the allowance of only "reasonable" charges) have traditionally been problematic to the medical records copying industry and the encompassing health care industry. The rationale for both of these findings is discussed below.

III. Controlling the Cost of Medical Records Copying

A. Understanding the Medical Records Copying Process

It is important to understand the steps involved in processing a request for health information when creating a mechanism for establishing and controlling the cost of medical record copies. Before describing the process, however, it is important to point out three overriding characteristics of the process. First, processing a request for health information is extremely labor intensive. Second, the personnel involved in this process are highly skilled in ensuring the continued confidentiality of health information. Third, utilizing a professional copy service results in a savings for the health care industry both in terms of time and costs.

Health information professionals recognize that more than 20 separate and distinguishable tasks are involved in processing a request for a single medical record. In general terms, these steps include:

- Receive and open request
- Log request
- Review authorization
- Locate medical record number
- Retrieve record:
 - Locate record whether on-site or off-site
 - Locate record whether in paper, computer, microfilm or optical form
- Ensure record is complete
- Match request with records retrieved
- Verify patient's signature
- Examine every page for confidential and/or legally protected information

- Designate information for copying
- Disassemble records
- Copy records and reports
- Reassemble records
- Prepare certification letter
- Prepare invoice
- Update record log
- Prepare copies for mailing
- Mail copies
- Refile record
- Prepare and enter billings
- Provide customer service

A detailed flow chart which graphically illustrates the medical record copying process has been attached as an appendix to this statement. As indicated by the flow chart, processing a medical record request is more complex than one would presume. But more importantly (for H.R. 4077's purposes), it involves a number of steps designed to ensure disclosure of only authorized information and protection of the patient's right to privacy.¹

B. Limiting Fees to "Actual" Cost

H.R. 4077, section 111(d), states that a health information trustee may charge a "reasonable" fee, which is defined as one not greater than the "actual" cost for providing a copy of protected health information. Similar limitations have been proposed at the state level. These initiatives are generally premised on a flawed comparison of the cost to copy medical records versus the cost to copy ordinary documents at a library or printing/copy store. The state legislatures which have reviewed this issue have generally found, however, that limiting the cost for copying medical records to their actual cost is an untenable proposition.

As described above, copying medical records is a time-consuming and labor-intensive service. Health information professionals also spend considerable time ensuring that only authorized information is released and that the privacy of individually identifiable information is protected. In addition, the health care provider or a copy service must invest in hardware and software for logging requests and status updates, copy equipment, microfilm reader-printers, storage space, postal costs, bad debt expense, etc.

When a customer uses a copier at the library or printing store, they have invested their own time in researching the materials and reproducing the copy. Because of the inherent differences between these two processes, conclusions drawn from a comparison of the local print shop's \$.10 copy and a medical record

¹ Please refer to the flow chart in the Appendix, steps 3, 12, 13, 14, 15, 16, 18, 24, and 31.

copy are flawed. Health care providers and medical record copy services should not be limited to the "actual" cost of duplicating a page.

C. Limiting Fees to "Reasonable" Cost

Imposing a "reasonable" fee limit on medical record copies serves an admirable public policy (i.e., preventing health care providers or copy services from charging an excessive price) but is problematic for the health care and copy industries. Several states currently have "reasonable" fee cost limitations. This standard is inherently vague and opens the door to litigious attorneys and class action lawsuits. Any cost savings sought by the proponents of a "reasonable" cost constraint are depleted by the cost of subsequent litigation to determine what is "reasonable." Smart Corporation has found that medical record copy charges should be based on clear and understandable criteria which are established at either the Federal or state level.

IV. Smart Corporation Looks Forward to Offering Alternative Legislative Language

Smart Corporation appreciates this opportunity to present its views on H.R. 4077. Smart looks forward to continued involvement in the Subcommittee's efforts to improve on the bill. More specifically, Smart would appreciate the opportunity to present alternative language to H.R. 4077, section 111(d), for the Subcommittee's use during refinement of the bill.

V. Contacts

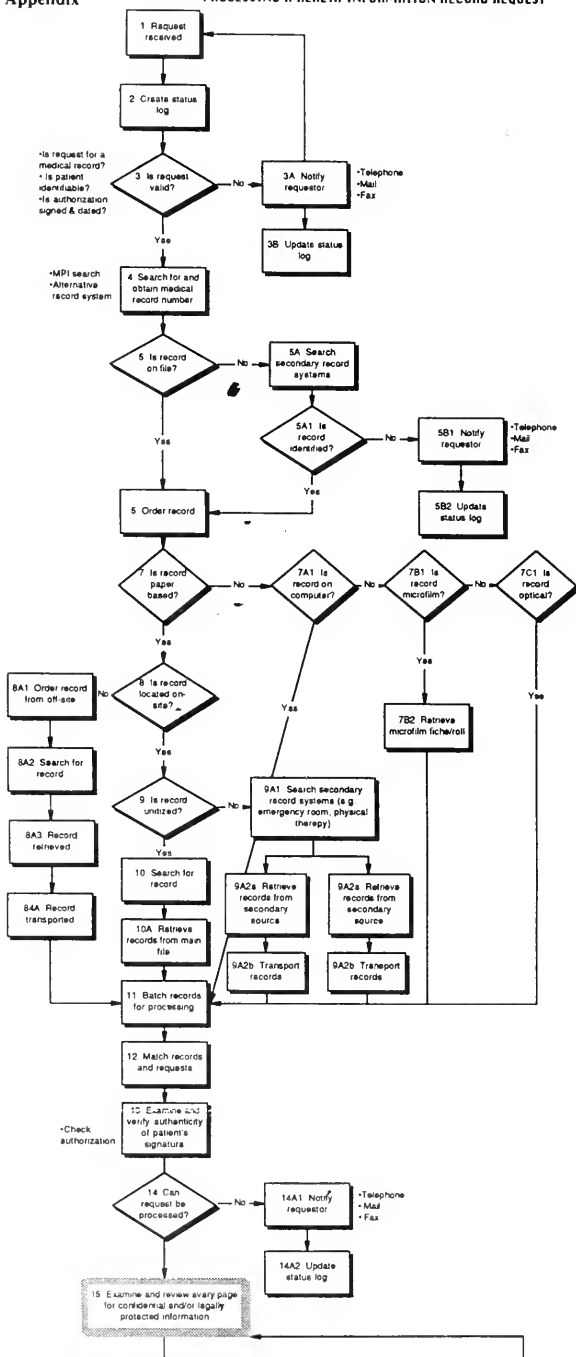
For further information, or to discuss alternatives to H.R. 4077, section 111(d), please contact either:

Peter D. Robinson, Principal
Bailey & Robinson
1201 Connecticut Avenue, NW
Suite 300
Washington, D.C. 20036
Telephone: 202-835-8810
Facsimile: 202-835-8891

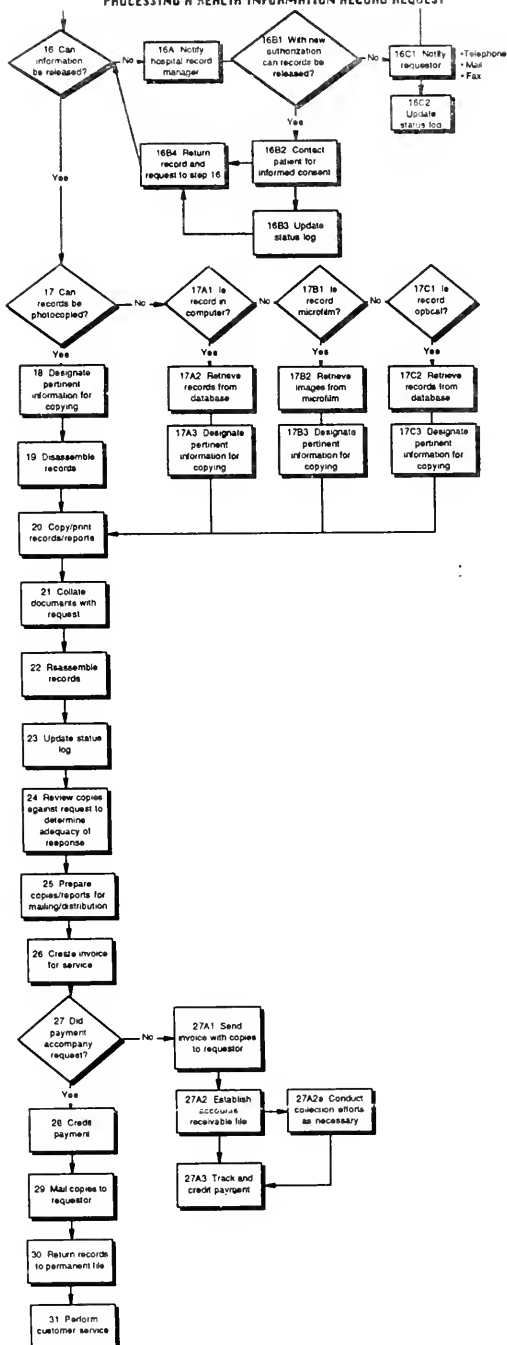
Christopher J. Mailander, Esq.
Bailey & Robinson
1201 Connecticut Avenue, NW
Suite 300
Washington, D.C. 20036
Telephone: 202-835-8853
Facsimile: 202-835-8891

V. Appendix

PROCESSING A HEALTH INFORMATION RECORD REQUEST



PROCESSING A HEALTH INFORMATION RECORD REQUEST





American Psychiatric Association

1400 K Street, N.W., Washington, D.C. 20005 • Telephone: (202) 682-6000

STATEMENT OF

THE AMERICAN PSYCHIATRIC ASSOCIATION

ON:

THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1994

H.R. 4077

Submitted To:

**The Subcommittee on Information, Justice, Transportation and Agriculture
of the House Committee on Government Operations**

May 20, 1994

The American Psychiatric Association (APA), a medical specialty society representing 38,000 psychiatric physicians nationwide, herein presents its recommendations on H.R. 4077, the Fair Health Information Practices Act of 1994.

We commend the author of this legislation. Congressman Gary Condit, Chairman of the Government Operations Subcommittee on Information, Justice, Transportation and Agriculture, and the original cosponsors of this bill, Congressman John Conyers, Chairman of the Government Operations Committee, and Congresswoman Nydia Velazquez, herself a victim of a most egregious breach of a patient's right to privacy, for introducing legislation designed to establish uniform federal guidelines for medical information. At the same time we are deeply concerned, because of the uniqueness of the need for absolute patient / psychiatrist confidentiality in the treatment of mental illness (including substance abuse), that the bill addresses limiting medical record disclosure, not prohibiting the event from occurring.

The name F. Scott Fitzgerald stirs thoughts of wealthy New York socialites enjoying glamorous parties at the Hamptons with exotic women who have names like Zelda. When a person thinks of Irving Berlin they are likely to start tapping their toes to "Alexander's Rag Time Band." The name Georgia O'Keefe is synonymous with abstract flowers captured on canvass mixing a beautiful harmony of color and light.

Fitzgerald, Berlin, O'Keefe -- all great artists -- all at one time in an asylum or psychiatric hospital.

Edna St. Vincent Millay, Sylvia Plath, William Faulkner, Ernest Hemmingway, Eugene O'Neill, Virginia Woolf, Joseph Conrad, Anne Sexton, Cole Porter, Jackson Pollock -- each had been in an asylum or psychiatric hospital, attempted suicide, or committed suicide.

Mental illnesses and substance abuse disorders do not discriminate by race, age, gender or ability. Today there are nearly 40 million adults in the United States who suffer from mental disorders or alcohol or other substance abuse. These 40 million Americans are entitled to have their medical records kept confidential.

As a Nation, and a people, we have entered the Information Age. We can communicate globally through a network of computers faster than we would have imagined only five or ten years ago. Reams of information can be downloaded in moments from system to system, enabling us to share valuable knowledge from city to city, coast to coast, and continent to continent. Yet, as with any form of progress, abuses, serious abuses, can and will occur. Sensitive, private material, has a market. It is a commodity -- to be bought and sold by those of questionable ethics.

Medical records, like any collection of data, are of value to various parties: on one hand, those such as doctors and patients, who have a legitimate interest in knowing and understanding what is contained in a patient's file; on the other hand, hackers and pirates, whose only interest is completely self-serving and often destructive; and there exists a gray area for third parties -- who have access to information for appropriate reasons, such as billing purposes, but the extent of that access, and what happens to the information once it is obtained by a third party, is of grave concern.

To reinforce why, as stated at the beginning, we express deep concern about the

legislation, because of the stigma associated with their illnesses, psychiatric patients are particularly concerned about preserving the confidentiality of this information. Many employees do not use their paid-for insurance benefits lest their careers be imperiled by their being labelled as psychiatric patients. Federal employees, armed-services officers, corporate executives and politicians often would realistically jeopardize their careers should their psychiatric treatment be disclosed.

We have recently witnessed what can occur when medical records, psychiatric records, are misused. Only weeks ago, local media covering the Republican senatorial primary race in Virginia focused on the mental health records of candidates James C. Miller, III and Oliver L. North. Psychiatric treatment had become a campaign issue -- used as a tactic to discredit the candidates, exploiting misguided prejudices about psychiatric illness and emotional distress.

Only last month newspapers in Pittsburgh, Pennsylvania headlined the story of a State Supreme Court Justice who was tried for using employees to obtain prescription drugs to treat severe depression. The defense argument was compelling: this was a legitimate means of avoiding negative publicity and preserving a legal career.

In testimony on this case, an internist and friend of the defendant testified that he assisted in covering up the justice's use of anti-depressant medication. As reported:

"We wanted to protect him," . . . He's had a longstanding problem [and] he deserves privacy."

The effort to conceal the justice's illness and prescription drug use reached the extent that [his internist] kept information out of [the justice's] medical file so nothing damaging could be leaked to the media by anyone who saw it.

"The files could fall into anybody's hands," he said.

"Who had access to the file?" asked . . . the first deputy attorney general prosecuting the case.

"The office girls and myself. . . Cleaning people could take it." 1

The need for absolute confidentiality, not limited disclosure of a medical record, can best be articulated by someone suffering from the stigma associated with mental illness. Accounts of the trial, as taken verbatim, follow:

Q: When in your lifetime did the pain inside get so great that you went for help?

A: After my second marriage, which was, you know, as -- after my termination of my second marriage, which was as traumatic as the termination of the first marriage, and I decided I wanted to get some help.

Q: How many years ago was that, Your Honor?

A: This was in the sixties. It would have been -- well, I don't know.

Q: Was it during that period in your life that you were told that you had a mental illness?

A: Yes. It was a Dr. Odo Mell, and I saw him twice a week, and he prescribed the first psychotropic drug I ever had which was Librium.

Q: How did you pay that doctor?

A: With money.

1. Gary Rotstein, Larson Doctor Justifies Rx Deal, Pittsburgh Post-Gazette, vol. 67, April 6, 1994, p. A. 1

Q: Cash?

A: Cash.

Q: Why?

A: You mean as opposed to insurance.

Q: Correct.

A: Because I wanted to keep it confidential.

Q: Why were you interested in the confidentiality of that diagnosis?

A: Because of the stigma of when you see a psychiatrist, you see a psychiatrist because you have mental illness. Even back then there was less understanding about mental illness than there is today.

Q: What is the stigma?

A: The stigma is that there is something the matter with you, something that people have an aversion to people that have mental illness.

It also goes to the consideration like I was a lawyer at that time, and I knew some day I wanted to go to judiciary.

In a sense, it's not fair to citizens because of the stigma, not because of the mental illness, but because of the stigma. If you know a judge or a jurist has mental illness, you may question because of the stigma, because of what we have been taught in society. It's a prejudice even though that Lincoln had depression. Lincoln is considered one of the greatest presidents we ever had. He would not be elected today because of his mental illness. He couldn't get the treatment I got.

There weren't any psychotropic drugs. Churchill had it. There were no psychotropic drugs. There weren't antidepressants until just modern times, and so in some senses it's not fair to the citizens for them to see a judge, a jurist, a doctor, maybe even your babysitter. Do you want somebody that's depressed or has anxiety, chronic? Your babysitter?

I'm working and I function fine, but there is that prejudice and there is that problem with professional people, and what's fair for you as citizens to have? 2

2. Larsen in His Own Words, Pittsburgh Post Gazette, vol. 67, April 8, 1994, p. A-11.

The efforts of the Clinton Administration, and the continuing efforts of the Congress, to reform the nation's health care system pose a unique opportunity for redressing discrimination against persons with mental illness (including substance abuse), for ensuring that persons with mental illness have access to care their illnesses require, and for safeguarding the confidentiality of their medical records.

The Health Security Act establishes a Health Information Network, created by the National Health Board, to collect and report a myriad of data. This key element of the Administration's Health Care Reform Proposal is designed to produce an electronic health information network. Individuals will carry Health Security Cards and have identification numbers. Information gathered on clinical encounters, agreements between health plans and health providers, payment of benefits, and utilization management will be used to evaluate costs, develop policy, and improve the quality of care. It is hoped that the application of our advanced technology will not only contain costs by reducing paperwork, but improve patient care by providing accurate, critical information in a rapid manner.

Preserving the confidentiality of the doctor -- patient relationship, not merely limiting the medical record, must be the cornerstone upon which this new system is built. The Administration's proposal requires that the National Health Board, two years after enactment, promulgate standards with respect to the privacy of an individual's health information, including safeguards for the security of such information. Three years after enactment, the Board is required to submit a federal legislative proposal to provide for patient medical record protection.

While the goals outlined in the Health Security Act are meritorious, the APA is pleased that the Fair Health Information Practices Act, H.R. 4077, seeks to address these essential issues now, as Congress debates the fundamental concerns of reforming our Nation's health care system.

If confidentiality is the fundamental premise of the doctor -- patient relationship, then it is the linchpin of the psychiatrist -- patient relationship. To avail oneself of psychiatric help, it is necessary that the most intimate and private thoughts be disclosed to the physician. Any interference with the maintenance of confidentiality of such communication impairs the ability of a psychiatrist to help his or her patient. Because the material disclosed to a psychiatrist includes information relevant to a patient's relationships to the whole outside world, the psychiatrist becomes the repository of information valuable to many third parties, such as insurance carriers, legal adversaries, law-enforcement agencies, and employers. To the extent that such information is disclosed without the patient's consent, the reliability of the physician-patient relationship is eroded, and the ability of a physician to help his or her patient is impaired.

It is necessary to draw a new balance between society's need to provide an ambience in which patients may be restored or helped to a state of maximum productivity and to provide access to information required by a complex society and its health care delivery system. Preserving medical record confidentiality, and protecting the privacy and security of sensitive personal information, is one of the hallmarks of APA's twelve Principles of Health Care Reform.

The welfare of the patient is the first concern of the psychiatrist. From this concern derives the psychiatrist's obligation to protect patients' privacy and maintain the confidentiality of their communications. In a world of utilization review, and third party payers, and likely under a reformed, computerized system of health care, it is increasingly difficult for psychiatrists to fulfill that obligation. We strongly recommend that any national health care proposal recognize that protecting the confidentiality of medical disclosures is especially imperative for those who need and obtain psychiatric treatment. Until a psychiatric patient can be assured that there is no stigma against this illness and no prejudice against themselves, it is clear that psychiatric records need an extra level of protection, and we urge the Committee's support for our recommendations to amend H.R. 4077 as outlined below:

Section 121-b (page 31)

This section permits disclosures of medical record information by the newly created "Health Information Trustee," those who are in a position to create or receive protected health information. Duties and potential penalties are imposed to ensure that only authorized, urgent, or legally required information is released. The intent of this section, however, is thwarted by codifying that third parties can legally disclose medical records or health information if doing so is consistent with the provisions of the bill outlined below. Health care providers, insurers, and health oversight agencies, considered trustees under this bill, can release information. For example, Section 111-b-1 does not require that the **treating physician** elect to release or not to

release mental health treatment notes. We recommend that the treating physician explicitly be designated as the person deciding if access to mental health notes should be denied.

Section 122-c-1 (page 35)

This provision prevents health care providers from requesting that patients authorize the release of medical record information on a day on which the provider renders health care to the individual, or on the day of admission to a medical facility. The underlying rationale for this prohibition may be a concern that patients may be coerced into signing authorization forms when such forms are offered to them concurrent with the receipt of medical care. This concern seems farfetched, and the practical difficulties likely to be engendered by this prohibition are substantial.

For outpatients, facilities and providers will be unable to request previous treatment records unless the patient makes a special visit, on which no health care is rendered, in order to provide such authorization. Inpatients would be rendered ineligible to provide such authorization throughout their entire hospitalization. Since medical history data is often crucial to making a diagnosis and formulating a treatment plan, this would represent a severe and unacceptable limitation on clinicians' ability to gather such information. Moreover, were Section 123-a-2, which authorizes unlimited release of information for insurance and other payment purposes, to be modified to be more protective of patients' interests as outlined below, this provision would effectively prevent patients from granting authorization for release of information to insurance

companies and managed care entities as well. **We recommend that this section be deleted.**

Section 123-a-1 & 2 (pages 39-40)

These sections would permit unlimited release of information without patients' consent to other health care professionals who are providing care to the patient, to insurers, and to managed care companies. Patients often have legitimate reasons for desiring that such information not be released. Their psychiatric records, for example, may not be at all relevant when they seek medical or surgical attention. In addition, psychiatric patients may elect to pay for psychiatric services out-of-pocket rather than release information to managed care companies, particularly if that information is likely to make its way back to their employer or union. **Thus, release for either of these purposes should be restricted to situations in which the patient is physically or mentally incapable of authorizing release, or in which the patient is unavailable (after efforts have been made to locate the patient) to be asked for permission.**

Section 124-a (page 40)

Release of health information to next-of-kin would be permitted in this section, as long as the patient had not previously objected to the disclosure. This is contrary to the standard of practice in psychiatry, where patient information is never released to family members without the patient's explicit authorization. Other medical information, for example, regarding substance abuse treatment or birth control, may be similarly sensitive. **The only situations in which an**

exception to the requirement for obtaining patient consent should be when consent is unobtainable because of the patient's physical or mental state, or in an emergency.

Section 124-b (page 41)

Under this provision, information regarding the identity of patients, their hospitalization status, and their general medical status would be releasable without consent. This would permit information regarding a patient's hospitalization to become essentially part of the public record. Yet, patients may have many legitimate reasons for not wanting other people to know that they have been hospitalized, whether for a physical or mental problem. Moreover, these provisions probably conflict with federal law on the confidentiality of alcohol and substance abuse treatment records (42 USC 290ee). **We recommend deleting this section.**

Section 127-b-1 (page 44)

This provision would permit a party to litigation in which a patient has placed his or her physical or mental condition in issue to request access to the patient's medical records. Release of this information could take place merely on receipt of a statement from the party desiring the information. Although this provision is designed to embody the "patient-litigant exception" to the privileged status of medical records, it does so in a way that completely disregards legitimate privacy interests. There is no mechanism for guaranteeing the validity of the request, or for notifying the patient of the request and allowing the patient to challenge the basis for release.

Persons desiring access to medical or psychiatric records of a party to litigation should make their requests to a court, with notice provided to the patient and an opportunity afforded for a hearing on the issue. Records should only be released after a court order has been obtained.

Section 129 - (pages 45-46)

The exceptions to the confidentiality of medical records afforded law enforcement agencies in this section are enormous in scope. Law enforcement agencies can request release of information for an investigation or prosecution of "a health information trustee", apparently not restricted to the trustee holding the records themselves. They can make similar requests to identify or locate suspects, fugitives, or witnesses, and even to determine whether a crime has been committed. Subsection "b" allows them to obtain this information merely with the signature of a supervisory official of the law enforcement agency itself. Thus, any medical record information can be released on the request of a law enforcement agency even in the absence of any reason to believe that a crime has been committed. This is extraordinary. Law enforcement agencies would be provided with unrestricted fishing licenses under this provision. Further, this section appears not to be governed by the extensive requirements of Sections 141 to 143 below. They afford patients the opportunity to challenge access to their records when a subpoena or warrant is issued for those records. As this section is written, it appears that law enforcement agencies can avoid any review of their request whatsoever by simply informally asking for the records, rather than by obtaining a warrant or subpoena. **No exceptions should**

be made to the requirements for warrants or subpoenas, with all the protection afforded by Sections 141 to 143 below.

Section 142-f (pages 55-56)

This section establishes the standard for a decision and the burden of proof regarding a patient's challenge to the right of a governmental agency to subpoena or obtain a warrant for medical record information. In order to discourage fishing expeditions, the burden should be on the government to prove that its need outweighs the individual's privacy interests, rather than the other way around. Moreover, the government should carry the burden of demonstrating that there is no other, less intrusive way of obtaining the information and to provide evidence suggesting that the information contained in the medical record is likely to be probative of the issue in question. Judges should be required to review the information in question in chambers and to permit redaction of material that is irrelevant to the purpose for which the warrant or subpoena is requested.

Section 143-c (pages 58-59)

Similar changes regarding the burden of proof and the absence of less intrusive means for obtaining the information should be made to this section.

APPENDIX 3.—HEALTH INFORMATION PRIVACY SURVEY 1993, CONDUCTED FOR EQUIFAX BY LOUIS HARRIS AND ASSOCIATES IN ASSOCIATION WITH DR. ALAN WESTIN, COLUMBIA UNIVERSITY

Section 156-b-2 (page 66)

This provision would permit parents or legal guardians to have unlimited access to the medical records of patients between fourteen and seventeen years of age. Since adolescents frequently discuss sensitive issues with their psychiatrist, including information that they would not like revealed to their parents, and exception should be written into this subsection for psychiatric and other mental health records.

We recognize that the intent of H.R. 4077 is to protect this Nation's citizens, but we respectfully point out the profound hazards to patients by allowing access to medical records contained therein. We also recognize that establishing security in an electronic health information network, as called for in the Administration's Health Security Act, will be a daunting enterprise.

HARRIS-EQUIFAX

**Health
Information
Privacy
Survey
1993**



Conducted for Equifax by Louis Harris and Associates
in association with Dr. Alan Westin
Columbia University

Study No. 934009

HEALTH CARE INFORMATION PRIVACY

A Survey of the Public and Leaders

Conducted for EQUIFAX Inc.

Fieldwork:

July 26 to August 26, 1993

LOUIS HARRIS AND ASSOCIATES
630 Fifth Avenue
New York, NY 10111
(212) 698-9600

© *Copyright 1993 Louis Harris and Associates*

TABLE OF CONTENTS

Page

A Message from Equifax.....	i
Introduction	1
Survey Highlights.....	2
Interpretive Essay by Alan F. Westin	5
Chapter 1: Personal Privacy in America Today	22
Chapter 2: Attitudes and Experiences of the American Public with Health Care and Medical Records	34
Chapter 3: Uses of Medical Information for Marketing and Research.....	42
Chapter 4: Disclosure of Confidential Information and Medical Records.....	47
Chapter 5: Information Technology.....	65
Chapter 6: Life Insurance	72
Chapter 7: Employment	82
Chapter 8: Health Care Reform.....	87
Chapter 9: The Issue of Personal Identity Cards and Numbers	93
Chapter 10: Privacy Legislation	97
Chapter 11: Leaders' Attitudes Toward Information and Procedures.....	104
Index of Tables	111
Appendix A: Survey Methodology	117
Appendix B: Questionnaires	121

A MESSAGE FROM EQUIFAX

The privacy of personal health information is a critical issue in national health care reform. It is apparent that any reform plan will involve new and increased uses of health information, new automated health care administration systems, and more personal identification of consumers in standardized formats. The handling of personal medical records and broader health information privacy issues will become primary concerns of virtually every American. For these reasons, we decided to sponsor this major new survey on the specific subject of health and medical information privacy.

We wanted to probe the attitudes of consumers, health care and business leaders toward such topics as — the level of trust Americans have in institutions that use their medical information; the need for privacy-protection safeguards; the use of medical information for marketing and research; the desirability of legislation; and the essential components of a national health care reform plan.

Now we have the results — including an analysis by Dr. Alan F. Westin, academic advisor to Louis Harris and Associates and a leading privacy expert — which should be of great interest to the many groups involved in health care as well as to the public at large. A number of findings are important to the overall national discourse on health care. For example:

- Most Americans favor reform of the current health care system. They want a reform plan that reduces fraud and abuse, reduces costs, and protects the confidentiality of medical records and health information.
- People generally believe their personal medical information is being protected by health care providers, but are concerned that increasing use of computers may result in improper disclosure of sensitive information.
- Most of the public favors enactment of comprehensive federal legislation covering health care information privacy.

The survey report also contains findings of particular interest to Equifax and other companies handling medical information:

- The American public wants businesses that handle sensitive medical data to have strong privacy, confidentiality, and security standards.
- The public favors the use of a personal identity card for health care purposes. If there is to be a personal identification number, most people prefer it to be the Social Security number.
- Most Americans find it acceptable for life insurance companies to obtain a wide range of health and lifestyle information, but almost half of the public expresses concern about employers' use of medical claims information.

These findings and others in this survey will add important knowledge to the resolution of health information privacy issues. The survey results will also provide a valuable road map for Equifax and other companies providing health care information services.

Equifax currently offers a portfolio of services relating to health care — including hospital bill auditing, accounts receivable management, claims administration, physical examinations, and analytical services.

As we provide services to help speed the processing of claims and the evaluation of insurance applications, we come in contact with personal medical information and have developed privacy policies governing how we handle such sensitive data.

As a company deeply concerned about information privacy, Equifax has a two-pronged objective: to understand the privacy concerns of individuals and to ensure that our practices involving the use of personal medical information reflect superior levels of sensitivity and security. With the help of expert consultants, we will apply the lessons learned from this study and our previous privacy surveys.

The challenge for us and for American society will be how to strike the proper balance between the collection, processing and analysis of medical data for high quality health care, cost control and fraud prevention — and the protection of sensitive, personal, medical information about individuals.

We hope that the information from this survey will promote a better understanding of important health care privacy issues and be of considerable value to the development of proper privacy protection as new health care approaches and information systems are developed in America.



C. B. Rogers, Jr.
Chairman and Chief Executive Officer

INTRODUCTION

Louis Harris and Associates was commissioned by Equifax Inc. to conduct a major survey of leaders' and consumers' attitudes regarding health information privacy (i.e., the privacy and confidentiality of personal medical records). The survey addressed a cross-section of the American public and a leadership sample consisting of executives, professionals, and state and federal officials in the health care field.

Between July 26 and August 26, 1993, interviews were conducted with a cross-section of 1,000 Americans eighteen years of age and over and with 651 leaders as described above.

A more detailed explanation of the sample composition is contained in the technical appendix. In this report the two principal groups of respondents are often referred to simply as "the public" and "leaders."

Statement Of Purpose

As national health care reform takes shape, one central component of the plan will be linked databases of medical information best symbolized by the Health Security Card displayed by President Clinton in his September 1993 address to Congress.

With this larger, integrated source of information comes the potential to detect fraud, to conduct outcomes research across a larger base of patients, and to develop practice pattern guidelines and improve the quality of care and reduce costs.

This survey specifically addresses privacy issues associated with health information and health care reform and is the fourth in a series of Equifax surveys on issues related to privacy in the information age.

Both public and leadership experiences with, and attitudes toward, the use of personal medical information in a variety of situations were explored in light of potential health care reform. Questions from the earlier Equifax surveys on general levels of concern about threats to privacy and the underlying sources of such concerns were also asked again.

Louis Harris and Associates is indebted to Dr. Alan F. Westin of Columbia University, our academic advisor to this survey, who has provided us with substantive guidance and expertise on the issues that have been addressed.

A Note On Reading The Tables

An asterisk (*) in a table signifies a value of less than one-half percent (0.5%). A dash (-) represents a value of zero. Percentages may not always add to 100 because of computer rounding or the acceptance of multiple responses.

Public Release Of Survey Findings

All surveys conducted by Louis Harris and Associates adhere to the code of standards of the Council of American Survey Research Organizations (CASRO) and the code of the National Council of Public Polls (NCPP). Because data from the survey will be released to the public, any release must stipulate that the complete report is also available.

SURVEY HIGHLIGHTS

Although the privacy of medical records may not be an issue to which the general public has given much thought, it has the potential to become a very important issue. Most Americans are deeply concerned about threats to their personal privacy in general and, when asked specifically, express concern about the possible misuse of confidential medical records. They believe strong laws are needed to prevent abuse. Other recent Harris surveys have shown that financial and medical records are the two areas where Americans regard privacy protection as most important.¹ Americans also want institutions which collect and use this information to have strong privacy protection policies.

Most people express confidence in their providers' use of their medical records, and only small minorities believe that their medical records have ever been improperly released. Their concerns focus not so much on their providers as on employers, insurers, government health officials or other analysts who might have access to their records. One reason for concern about medical records privacy appears to be the perception that increased computerization will make their records more accessible to more people for more purposes.

Leaders, however, see many ways in which the use of medical records in analysis can help improve the quality of care: through outcomes research, practice guideline development, and practice pattern analysis, while reducing the cost of care through detection of fraud and abuse. The cost of care could also be reduced through a reduction in paperwork.

The following are some of the specific findings of this survey:

A. Attitudes Toward Privacy In General

1. The high level of public concern about general, unspecified threats to its privacy, having risen more or less steadily up to 1990, has remained stable over the past three years. However, that level is indeed very high; fully 80%² are very or somewhat concerned about "threats to [their] personal privacy in America today." Recent Harris Poll data has shown the degree of concern was as high as 83% over the period between April and June of this year. This modest upward blip may possibly be explained by the higher levels of public discontent experienced during this period with the President, the Congress and "the system" in general. Blacks, Hispanics, women, and liberals all register above average levels of concern.

2. The leadership groups surveyed also register very high levels of concern about their personal privacy, although somewhat lower than that of the general public.

Physicians and state legislators show the highest levels of concern.

¹Harris Survey for *Privacy and American Business*, April, 1993

²When 49.3 very concerned and 30.3 somewhat concerned are added together, and rules of rounding applied, the total of the two responses is actually 80%.

3. Feelings of distrust among the public toward business, technology, and government have increased since 1990.

The leadership groups are much less distrustful in their attitudes about technology and business than the public is, and business is less distrusted by both the public and leaders than government and the political process.

B. Attitudes Toward Privacy Of Medical Information In General

1. A large majority of the public believes that it is very important that they should have the legal right to obtain their medical records. One-quarter of all those with a regular source of care have asked to see their medical records. In almost all such cases (92%), people were given their complete records and said they could understand them.

2. The majority of Americans do not find it acceptable to have their medical records used without their consent for direct mail related to new medications, medical research or a hospital fund raising. Most people (60%) feel it would be unacceptable for pharmacists to provide pharmaceutical companies with the names of customers using certain medications for use in direct mail. Slightly more people (66%) feel it would be unacceptable for hospitals to use the names of patients to solicit donations. Sixty-four percent also state that their permission should be required before their records could be used in medical research, even if no personally identified information about them were published.

3. While most Americans (73%) say that nobody has ever disclosed improper medical information about them, a sizeable minority (representing 50 million people) believes that their own medical records have been improperly disclosed.

The agencies most often seen to have violated the confidentiality of medical records are health insurers (15%), hospitals or clinics (11%), public health agencies (10%) and employers (9%).

One in three of the people (about 15 million people) concerned say they were embarrassed or harmed by these improper disclosures.

4. More than half of the leaders believe that violation of the privacy of medical records is a somewhat serious problem today.

Nurses and physicians are the most likely to believe this is serious.

5. There is very strong support for requiring information-processing organizations which handle medical records to have detailed privacy protection policies.

Majorities of the public and of leaders believe this is very important and that organizations should be selected on the basis of their proven record in protecting the privacy of the information they handle.

6. There is widespread acceptance that insurance companies need to ask for a broad range of health-related information from people applying for individual life insurance.

This is true both for the public and leaders and covers such topics as testing for illegal drug use, and HIV/AIDS, medical history, alcohol and tobacco use, and engaging in dangerous sports.

7. Most people believe that strong laws exist today to protect the confidentiality of medical records. This is not the view of most experts, who generally believe that there is only limited state and federal legal protection.

8. The great majority (87%) of Americans believe that the health professionals they see can be trusted to keep their records confidential and not misuse them.

C. Health Care Reform

1. Most people believe that health care reform will involve more record keeping and more computerization of medical records. This belief is a cause of anxiety because of the public's concern that computerization will allow more people to have easy access to medical records for more purposes.

2. A large majority of the public (84%) finds the idea of a personal health insurance card acceptable for use in administering a national health care system. This probably reflects support for the concept of universal access and security in relation to health insurance coverage. However, when asked about having a national health insurance number assigned to each individual, as part of health care reform, many people are very concerned (28%) or somewhat concerned (29%) about having a number assigned to them.

More people would prefer to have their Social Security number used rather than have a separate health insurance number.

3. Large majorities of the leaders believe that various uses and analysis of medical records will help improve the quality of care and reduce costs through outcomes research, practice pattern analysis, the development of practice guidelines and the reduction of fraud and abuse.

D. Legislation And Regulation

1. When asked about it directly, a majority (56%) of the public favors new, comprehensive federal legislation to protect the privacy of medical records as opposed to continuing with existing state and federal laws and professional standards. This response may reflect a desire for strong privacy protection and the belief that, with federal health care reform, protecting the confidentiality of medical records by national law seems appropriate.

2. A variety of proposals for what might be in a federal law all trigger strong positive responses. Overwhelming majorities think it is important that:

- penalties be imposed for unauthorized disclosure of medical records.
- rules be drawn up as to who has access to medical records and what information can be obtained.
- people can inspect their own records and have a procedure for correcting them.

A substantial majority also favors the concept of an independent national board to issue regulations and enforce standards.

INTERPRETIVE ESSAY: Dr. Alan F. Westin

Purpose and Scope	6
Overview of the Survey and the “Health Information Privacy Data Set”	6
Three Zones of Personal Health Information Use	7
Zone 1 — Direct Health Care	8
Zone 2 — Health Care Support Activities	9
Zone 3 — Societal Uses of Health Information	9
Summary of the Main Findings	10
How Personal Experiences and Conditions Affect Medical-Privacy Positions	12
Users of Mental Health Services	12
Adverse Physical Health Conditions	12
People Without Health Insurance	13
Adverse Medical Confidentiality Experience	13
How Demographic Divisions Affect Medical-Privacy Positions	14
How Attitudinal Orientations Affect Medical-Privacy Positions	15
Distrust Index	16
Computer Fear Index	16
Medical Information Sensitivity Index	17
How Many Americans Are Strongly Concerned About Medical Privacy?	18
General Concern about Privacy	18
Consumer Privacy Concern	18
Medical Privacy Concern	18
Public and Leaders Compared	19
Implications for Health Care Reform and Health Information Systems	20

Purpose and Scope

I appreciate this fourth opportunity to serve as academic advisor to a Harris national privacy survey sponsored by Equifax and to contribute an essay interpreting the survey findings. My essay will:

- present an analysis of the flows of medical and health information in American society today as a framework for the survey inquiry into medical privacy issues;
- provide a summary of the survey's main findings about public attitudes toward medical and health information issues;
- explore factors that seem to underlie public attitudes toward health information privacy issues;
- bring together and analyze demographic and other group patterns;
- compare public and leader attitudes on health information privacy; and
- consider the implications of these findings and explanations for the handling of health information privacy issues in national health care reform.

Overview of the Survey and the “Health Information Privacy Data Set”

The Harris/Equifax 1993 survey asked a representative sample of 1,000 members of the public 100 questions, 90 of these on substantive matters and 10 on respondent demographics. Our Leaders sample of 651 persons was asked 75 substantive questions.

In the Public sample, five questions dealt with privacy in general terms; seven with the respondents (or family's) medical condition; and 14 with the respondent's (or family's) personal experiences with uses of health information. Thirty-nine questions dealt with attitudes of the respondent on the following topics:

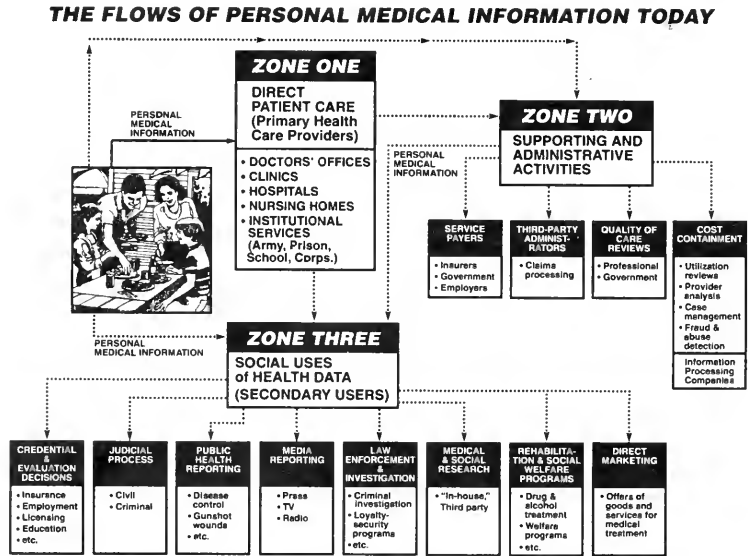
1. Issues of medical confidentiality and privacy (7)
2. Use of medical information in life insurance underwriting (8)
3. Uses of computers in health care (9)
4. Policy preferences on health information uses and privacy (7)
5. Issues of legal protection and regulation (8)

I have used these 39 questions as a “data set” to analyze the structure and sources of public opinion in 1993 on health information privacy issues. A matching subset of 24 questions asked of both the public and leaders has been used to analyze leader opinions and to compare public and leader attitudes.

Before presenting those analyses, however, some brief background is needed on the current flows of health information in American society.

Three Zones of Personal Health Information Use

During the past several decades, medical and health information has increasingly moved out of the offices of health care providers and into the record systems of a variety of non-providers. These flows of information are illustrated in the chart below.*



* The three-zone analysis was originally presented in Alan F. Westin, *Computers, Health Records, and Citizen Rights*, Washington, D.C.: U.S. National Bureau of Standards, 1976. Activities in the three zones (and the chart originally presented) have been updated to reflect new developments into the 1990's.

Zone 1— Direct Health Care. Zone 1 represents the settings where individuals go to get help from a health professional, whether in a physician's office, a clinic or hospital, or in the health unit of an institution (school, college, corporation, etc.). Three of four Americans (76%) report in our survey that they have a particular place they go when they are sick or need advice about their health.

Though conflicts of loyalty can arise when a health professional that the individual consults also works for a larger, non-health-care institution (such as an employer), the ethic of medical confidentiality generally operates in Zone 1 settings. This is usually reinforced by law through statutes and judicial decisions governing disclosure of patient information by health professionals.

Previous Harris surveys have shown that the public has very high confidence that doctors treat their patients' medical information confidentially and seek only the personal information they need to provide good medical care. Hospitals were also fairly high in the public's confidence.* In 1993, 87% of the public said they believe the health professionals they use are careful to keep their medical information confidential and not reveal it improperly.

Three trends in the 1980's and early 90's have significantly affected Zone 1.

- First, more sensitive personal information is being put into medical records today, such as mental health diagnoses and emotional-condition notations; alcohol and drug use data; genetic information, and sexual practices. This has made many Americans more concerned about who is looking at their medical records and where record information goes.
- Second, more health care treatment and service is being applied by persons other than physicians — nurses, physical therapists, paraprofessionals, and others. This expands knowledge of medical conditions and social data beyond the traditional physician-patient ethical relationship, and spreads such information among a widening circle of care givers.
- Third, increasing use is being made by health care providers of computers for billing and accounting functions, lab reports, and patient records. This is already a source of public concern. Half the public in 1993 say they are concerned today about computer uses by the providers from whom they get health services. Majorities in the 60-75% range see mistakes in charges, errors in recording medical information, and medical information being given to people who are not supposed to see it as events that are happening somewhat often to very often today "because computers are being used by health care providers."

* *The Dimensions of Privacy*, A National Opinion Research Survey of Attitudes Toward Privacy, conducted by Louis Harris Associates and Dr. Alan F. Westin for Sentry Insurance, 1979; *The Equifax Report on Consumers in the Information Age*, a National Opinion Survey conducted for Equifax Inc. by Louis Harris and Associates and Dr. Alan F. Westin, 1990.

Zone 2 — Health Care Support Activities. Zone 2 covers the acquisition and use of medical information for payment of services, quality-of-care reviews, and administrative controls. Private health insurance firms, self-insuring employers, and state and federal health program agencies are the core organizations needing to see individually-identified medical information in Zone 2. They use such information to verify eligibility and coverages; assess and pay reimbursement claims; and detect provider fraud. Increasingly, individual records are used to compare provider conduct in individual cases against practice guidelines and to create regularly up-dated databases of individual medical records to perform statistical cost-benefit analyses. A recent trend has been the entry into such health data operations of information-service companies or regional health consortiums that process medical claims and do analytical studies for employers and health insurers, adding another set of organizational players into Zone 2.

While few persons would challenge the need for and legitimacy of payment-review, quality-assurance, and anti-fraud activities, there has been growing nervousness on the part of patients and health care providers about the scope and amount of personal information required by Zone 2 organizations. Partly, these concerns arise because Zone 2 organizations are making coverage and reimbursement decisions that can result in denials of payment to individuals or providers or denial of treatments altogether. This creates tension over the depth and the propriety of personal information used to determine reimbursement or to assess treatment needs. This is especially true where documentation of mental conditions, alcohol and drug use, sexual practices, HIV status, and similar sensitive matters are involved, and where society's standards as to disqualifying or stigmatizing conditions for receiving health care are under debate. In the 1993 survey, one in four respondents (25%) — representing 46 million Americans — report that they or a member of their immediate family has personally paid for a medical test, treatment, or counseling rather than submit a bill or claim under a health plan or program.

At the same time, privacy boundaries are deeply involved in Zone 2 operations. A significant percentage of individuals in 1993 believe that Zone 2 organizations have disclosed personal information from their medical records in ways that these individuals consider improper.

Zone 3 — Societal Uses of Health Information. Individual medical and health information has come to be required for a wide range of societal activities — as a qualification or credential for private and governmental opportunities, as a relevant piece of information for many benefit programs, and as an appropriate matter for public disclosure, even without the individual's consent. As the chart shows, these societal uses range from employment, life insurance, education, and government licensing to civil and criminal judicial proceedings, rehabilitation and social-welfare programs, public health investigations and reporting, medical and social research, law enforcement, and news reporting to the public.

How to set the proper balance in each such area between the legitimate need for access to individual health information and the protection of confidentiality and privacy rights in health information is becoming a critical — and increasingly visible — issue in national privacy debates.

Concern over the uses and potential misuses of personal health information is increasing as more and more medical and health records go into computerized databases and are electronically exchanged among Zone 2 and Zone 3 organizations. How Zone 3 organizations acquire and use personal health information promises to be a significant issue in national health care reform efforts. Sixty-one percent of the public report that they are concerned that their medical information is being seen today by many

organizations beyond those the individual uses for health care services.

With this picture of the expanding flows of medical and health information in American society today from primary care into supporting activities and societal uses, and having noted briefly the different types of privacy issues in each zone, I turn now to a closer analysis of the 1993 survey results.

Summary of the Main Findings

The 1993 Harris/Equifax survey found the public to hold the following views relating to privacy and uses of medical information:

- **Confidentiality of medical information is an important matter.** Eighty-five percent say that protecting the confidentiality of people's medical records is absolutely essential or very important in national health care reform; they put this priority even ahead of providing health insurance for those who do not have it today, reducing paperwork burdens on patients and providers, and providing better data for research into diseases and treatments.

- **There is high trust in the confidentiality practices of those providing direct care.** As already noted, 87% of the public in 1993 believes the health providers they use are keeping their medical information confidential. And, only very small percentages cite any health service providers — doctors, hospitals, or pharmacists — when listing organizations that they believe have disclosed their personal medical information improperly.

- **But there are concerns about how medical information is circulating beyond direct care.** Forty-one percent are worried that medical claims information submitted under an employer health plan may be seen by their employer and used to affect their job opportunities; and 60% believes it is not acceptable for medical information about them to be provided, without their individual approval, by pharmacists to direct marketers who want to mail offers to new medications. Almost two of three Americans (64%) don't want medical researchers to use their records for studies, even if the individual is never identified personally, unless researchers first get the individual's consent.

- **Increased uses of computers by direct care providers has the public worried.** Half of the American public (50%) says they are concerned that their health care providers use computers today in managing their accounting and lab work and keeping medical records. Strong majorities feel that such computer use is causing mistakes to be made in charges (75%); mistakes in medical conditions to be put into patient records (60%); and medical information to be given to people who aren't supposed to see it (64%). Three of four Americans in our survey (75%) said they were concerned "that a computerized health care information system will come to be used for many non-health care purposes," with 38% of the public saying it is *very* concerned about this.

- **However, the public supports relevant and appropriate societal uses of health information.** In a test of such attitudes, large majorities of the public — from 62-81% — say it is acceptable for life insurance companies to collect medical or health-related information to decide whether to issue a policy to applicants and at what rate. Obviously, respondents felt the information items listed were all relevant and appropriate to use for life insurance underwriting purposes. Acceptable information included whether applicants drink alcohol, smoke tobacco products, or engage in dangerous sports; the applicant's medical history of past diseases and illnesses; and the applicant's family history of inheritable

conditions. The public also believes it is acceptable to require urine tests to detect illegal drugs and blood tests for AIDS or the HIV virus.

- **Attitudes toward national health care reform and enhanced uses of medical records are generally positive.** Eighty-nine percent of the public says that reforming health care is one of the top domestic issues facing the nation today. Seventy-six percent believe that record keeping will have to be increased and advanced computer technology applied if we are to manage health care reform efficiently, and a similar 76% says such computer use to administer a national health insurance system is acceptable to them even though it will mean handling individual medical records. However, a similar 75% worry that medical information from a computerized national health information system will be used for many non-health purposes. Overall, 54% of the public believes that “a person’s medical privacy in a national health care system will probably be protected better than it is currently.”

- **How to handle identification in health care reform is a troublesome issue.** A very heavy majority of the public (84%) says that it is all right to issue a national health insurance card to everyone for accurate identification and to administer the system. Although 57% report they would be concerned if everyone were assigned an identification number for the health insurance system, two out of three persons (67%) would prefer that it be their existing Social Security number rather than a new number just for national health insurance.

- **Strong majorities favor the passage of laws to safeguard medical confidentiality and patient rights.** The public is virtually unanimous — 96% — in saying that it is important that individuals have the legal right to obtain a copy of their own medical record. And, even though 67% believe there are already strong laws protecting the confidentiality of people’s medical records, 56% of the public say that comprehensive federal legislation is needed to accompany national health care reform to “spell out rules for confidentiality of individual medical records in such a system.”

- **There is high agreement on what should be in such national medical privacy legislation.** Ninety-six percent of the public believes any federal legislation enacted should designate all personal medical information as sensitive and impose penalties for unauthorized disclosure. A similar 96% support rules spelling out who has access to medical records and what information can be obtained. Ninety-five percent favor legislating a right of access by individuals to their medical records in the system, and creating procedures for updating or correcting such records. Finally 86% of the public favors creating an “independent National Medical Privacy Board to hold hearings, issue regulations, and enforce standards.”

- **The public wants medical-information-processing companies to have strong privacy policies.** Eighty-three percent of the public says it is important that the information-processing companies hired by government agencies, employers, and insurers to review individual medical records for analyzing treatments, results, and costs should have “detailed privacy and confidentiality policies.” In fact, 94% of the public feels that such organizations should be selected “on the basis of a proven record of protecting the confidentiality and security of the personal records they handle.”

While these findings as to public attitudes toward health-information-privacy issues are important in themselves, additional insight can be obtained from seeing which groups within the public are most (or least) concerned about medical privacy and in exploring the underlying causes of high concern.

Three sets of factors were analyzed in search of the sources for public divisions on medical privacy issues: personal experiences or conditions; demographic breakdowns; and attitudinal orientations.

How Personal Experiences and Conditions Affect Medical-Privacy Positions

Users of Mental Health Services

Twenty-two percent of the public, representing about 40 million people, report that they or a member of their family has used a psychologist, psychiatrist, or other mental health professional. Demographic groups scoring higher than the public in use of mental health services include post graduates (36%), people with incomes over \$75,000 (38%), residents of the East and West (28%), 18-29 year olds (31%), liberals (31%), independents in party affiliation (32%), and voters for Perot in 1992 (34%). Users of mental health services are lower than non-users in worries about computer utilization in health care or health care reform and in general distrust of institutions. However, they score higher than non-users in their general privacy concerns and in favoring strong legal protections of medical privacy.

Users of mental health services score significantly higher than non-users on issues relating to the handling of sensitive medical information. For example, they are higher in

- believing doctors and hospitals have disclosed personal medical information about them improperly and that they were harmed or embarrassed by that action;
- saying they did not seek medical treatment to avoid jeopardizing opportunities;
- paying bills to avoid submitting medical claims;
- worried about losing health insurance if they change jobs;
- opposing direct marketing uses of medical information without prior consent;
- doubting that health care reform will improve protection of medical privacy;
- favoring a legal right for patients to see their medical records;
- preferring a new health identification number over use of the Social Security number;
- favoring comprehensive federal legislation on medical privacy; and
- approving the selection of medical-information-processing organizations on the basis of their track record in protecting privacy.

Users of mental health services — almost one in four members of the public plus additional members of their families who may have used such services — clearly constitute one of the most high-concern segments of the public on issues involving the handling of sensitive medical information.

Adverse Physical Health Conditions

Thirty-five percent of respondents report that they or an immediate family member has had a serious illness such as a heart attack, stroke, or cancer; 19% have had a long-term condition such as diabetes or epilepsy; and 14% have a major physical or mental disability. Eliminating persons with more than one such answer, 55% of the public report that they or a member of their immediate family has what can be called an adverse physical health condition.

We tested whether persons in families with adverse physical health conditions might be more privacy sensitive than persons without such conditions. This was based on the premise that providing

information about these conditions and having their presence used in Zone 3 societal decision making might give such respondents a special outlook. This did *not* prove to be the case in the overwhelming majority of the 39-question set. Persons with adverse physical health conditions scored about the same as those without such conditions on almost all the questions used for our pattern analysis.

People Without Health Insurance

When presented with a list of possible health payment plans or programs, ranging from plans at work or health insurance purchased to coverage through Medicare or Medicaid, 13% of respondents — representing 24 million Americans — said they had no such coverage for health care services. Demographic groups high in this category include people with \$15,000 income or less (30%); less than high school education (22%); people 18-29 (21%), living in the South (17%) or rural areas (18); and Hispanics (18%).

The uninsured scored higher in privacy orientations than those who do have health insurance on 21 of our 39 questions. These answers occurred in the attitudes, experiences, and policy preferences areas of our question set. However, the uninsured scored *lower* than the insured in favoring legal measures to protect medical privacy or patient rights of access.

Adverse Medical Confidentiality Experiences

As noted in the findings summary, 27% of respondents (representing 50 million adults) report their belief that an organization or person having their personal medical information has disclosed it improperly. This is a dramatic finding, both in terms of how many Americans believe this has happened to them and also in the sense of violation of core privacy rights that these reports of improper disclosure document. Thirty-one percent of these respondents (representing 8% of the total population and 14 million Americans) go on to report that they were harmed or embarrassed by that disclosure.

Such "harmed by improper disclosure" persons represent what we call people with adverse medical confidentiality experiences. As group, they *scored higher than the rest of the public on 35 of our 39-question set, or 90% of the items!* Furthermore, the "point spreads" in privacy orientation between these persons and the general public were quite large, often in ranges of 15 percent or more.

Demographically, this group has higher concentrations among those who are high school grads but also those with post-college-graduate education; people in the \$50,000 and over income bracket; males; 18-29 year olds; and voters for Perot in 1992.

Do these beliefs in improper disclosure have a high paranoia content and should these self-reports be substantially discounted? Not if we look at several key responses by the leaders surveyed in 1993. When asked whether they are aware of violations of the confidentiality of medical records from inside organizations, 24% of the leaders said they did know of such violations and could describe them in detail. The 24% figure is obviously quite close to the 27% of the public reporting this has happened to them. In addition, almost three out of four leaders (71%) think the public *is* concerned about threats to the confidentiality of medical records, and 59% of the leaders themselves think violations of medical record confidentiality in America today is a serious problem.

How Demographic Divisions Affect Medical-Privacy Positions

Based on the answers to the 39-question set of substantive items about medical privacy and health information issues, how does the public divide in terms of demographic groups in the population. The chart below arrays each major demographic category into high, medium, and low medical-privacy concerns. (We also include at the end of the chart the placement of groups according to experiences, conditions, and attitudes.)

Levels of Medical-Privacy Concern Among The Public

High Concern	Medium Concern	Low Concern
Less than high school education; post-graduates	High-school graduates; some college	College graduates
South and East	West	Mid-West
Liberals	Conservatives	Moderates
Rural	Central city	Suburbs
\$15,000 or less; \$50,000 and over	\$15-\$5,000	\$35-\$50,000
Females	Males	-
Blacks and Hispanics	Whites	-
50-older	18 - 29	30 -49
Democrats	Independents	Republicans
Clinton and Perot voters, 1992	-	Bush voters, 1992
Used mental health services	Adverse physical condition	No adverse physical condition or use of mental health service
Medical info. disclosed improperly	-	No medical info. disclosed improperly
No medical insurance	Have medical insurance	-
High computer fear	Moderate computer fear	Low computer fear

While many of these distributions track attitudes on other social issues and are probably familiar to readers, several of the divisions deserve a word of explanation:

Those with *both* the lowest education and lowest income constitute about 9% of the public, or about 17 million persons. While whites make up the majority of this combined group, a third of all Blacks report \$15,000 or less total annual household income. Blacks are generally among the highest concerned groups on medical – and other – privacy issues. Harris/Equifax surveys in 1990, 1991, and 1992 have shown low-income, low-education, and minority-racial groups to be among the most highly concerned about general privacy threats, violations of employee and consumer privacy rights, and government invasions of citizen privacy in law enforcement and social-program administration. It is not surprising, therefore, to find these sectors of the public scoring “high concern” on medical-privacy issues in the 1993 survey.

On one demographic grouping involving income and education, however, a surprising pattern did develop. Respondents with the *least* and the *highest* education, and those with the *highest* and the *lowest* incomes, displayed comparable high concern on many of the 39 questions in our health information and privacy set. Since those with the highest incomes and education do not generally register high concerns on general-privacy, consumer-privacy, or employment-privacy issues, why do they display high medical-privacy concerns?

The answer may lie in the fact that high-income and high-education groups are among the heaviest users of mental health services and also report having their medical information improperly disclosed at rates much higher than the public. It may be that such respondents feel capable of defending their informational interests quite well in the employment and consumer contexts, and feel a part of the governing elite as far as general privacy concerns are involved. But, their use of mental health services and their adverse medical confidentiality experiences make them feel sensitive — and vulnerable — when medical and health information is involved.

How Attitudinal Orientations Affect Medical-Privacy Positions

In addition to identifying the most privacy-oriented segments of the public based on experiences or conditions, or on demographic group membership, we wanted to see what sets of attitudes produce highly privacy-oriented segments of the public, and how large this “attitudinal group” would be. As in earlier Harris/Equifax privacy surveys, we created a series of indexes based on the sample’s answers to 3 or 4 selected questions in a particular area, such as attitudes toward computers or distrust of institutions. Depending on how often a respondent took the “high privacy position” on each of the selected questions, we divided the public into three categories — high, medium, or low.

We then tested this three-fold division of the public by seeing how each group of respondents answered the 39 questions involving medical-privacy issues. If the high group of respondents took the most privacy-oriented position on most questions, the medium group took a less privacy-oriented position, and the low group took the least privacy-oriented position, this would suggest that the dimension we tapped might be a significant factor in explaining the underlying source of public views on all (or a subset) of medical-privacy issues.

Distrust Index

In 1978 and 1990, the Harris privacy surveys found a direct and strong relationship between level of distrust among respondents and their positions on the privacy issues presented in those surveys. (How the Distrust Index was created and what constitutes High, Medium, Low and No Distrust positions is explained in the 1993 Harris/Equifax Report.)

In our 1993 survey, the Distrust Index produced a strong correlation between a respondent's distrust level and his or her privacy views on five questions exploring general privacy concern — overall threats to personal privacy, consumers losing all control over circulation of their personal information, existing laws and policies on privacy not being adequate, etc. But, the Distrust Index produced strong correlation between distrust level and privacy orientation on only a small minority of the 39 question set dealing with medical and health privacy issues.

This may be because persons who generally exhibit low or no distrust have relationships to health information that cause them to be more sensitive on medical-privacy issues and thus to break from the normal distribution of privacy concern from highest to lowest according to distrust level. This seems to have happened because members of Low or No Distrust groups have had personal experiences with improper disclosure of their health information or are users of mental health services or are apprehensive about employer use of adverse medical information.

What this analysis demonstrates is that — unlike general privacy attitudes or attitudes on consumer affairs — low distrust of institutions is not necessarily a determining factor in people's attitudes on most medical-privacy issues.

Computer Fear Index

Previous Harris surveys (Sentry, 1978; Equifax 1990; Equifax 1992) have shown that the more a person regards computer applications as fostering too detailed data collection, exchanging information too widely, and failing to follow tight security controls, the more privacy oriented that person will be and the more favorable to regulation and legislative controls to limit computer use in the interests of privacy protection.

To test this factor in the medical-privacy area, we created a Computer Fear Index based on the following three answers:

- **Agree strongly** that if privacy is to be preserved, the use of computers must be sharply restricted in the future (40%);
- **Very concerned** that their health care providers are using computers today (18%); and
- **Worried a great deal** that computers will be used to handle individual medical records in health care reform (23%).

Those with 2 or 3 such answers were rated as high in computer fear; 1 answer as medium; and no answers as low. The public divided into three groupings as follows:

High Computer Fear	22% (representing 41 million Americans)
Medium Computer Fear	32% (representing 59 million Americans)
Low Computer Fear	47% (representing 87 million Americans)

Those scoring higher than the 22% High average were persons with the lowest education (37%); the lowest incomes (33%); 65 and older (33%); and minorities (Hispanics at 32% and Blacks at 29%). Persons in the High Computer Fear category also scored High in general concerns about privacy and in having adverse medical confidentiality experiences.

The Computer Fear Index worked on 28 of 37 questions involving medical privacy (2 questions were used on the index itself). In those 28 questions, the higher on the Computer Fear Index, the more privacy oriented were the respondent's answers. This tells us that people's general levels of comfort or discomfort toward organizational uses of computers is a significant underlying factor in shaping their views on most medical-privacy issues.

Medical Information Sensitivity Index

While our Computer Fear Index worked, we wanted to see whether combining fears about computers with sensitivity about circulation of medical information would identify another consistently privacy-oriented subset of the general population. If so, we would be able to see which demographic groups and experiences or conditions of respondents characterized this segment.

We did this by creating a Medical Information Sensitivity Index, based on respondents' answers to two computer-fear and two sensitivity-of-information questions, as follows:

- **Agree strongly** that respondent is concerned that his/her medical information is being seen today by many organizations beyond those used for health care services (32%);
- **Very concerned** that the health care providers respondents visit are using computers (18%);
- **Worry a great deal** that computers will be used to handle individual records in national health care reform (23%); and
- **Very concerned** about people being issued a health identification number for health care reform (28%).

If a respondent answered 3 or 4 questions with the strongest privacy position, he or she went into the High category; 1 or 2, into the Medium category; and no strong-privacy answers into the Low category. Dividing the public into these three groups produced the following distribution as to Medical Information Sensitivity:

High	13% (representing 24 million adults)
Medium	45% (representing 85 million adults)
Low	42% (representing 78 million adults)

This Index proved to be strongly correlated with privacy orientations on a large majority (over 75%) of the items on our health information privacy question set). Those scoring highest took the most privacy-oriented position on substantive questions; Medium took middle positions; and Low were the least privacy oriented. There were also substantial spreads in percentages among the High, Medium, and Low positions.

This index illustrates that combining people's attitudes toward organizational uses of computers and concern over handling of medical information and a national identification number produces an attitude set that strongly influences people's views on medical-privacy issues.

How Many Americans Are Strongly Concerned About Medical Privacy?

In earlier Harris/Equifax surveys (1990, 1991, and 1992), we analyzed public responses to sets of questions about privacy in general and a variety of consumer privacy issues and created two indexes similar to the ones described above:

- **General Concern About Privacy**

Our index found that 25% of the American public scores High in general privacy concern; 18% scores Low; and 57% are Medium. We termed the High 25% to be “Privacy Fundamentalists,” seeking sharp limits on organizational data collection and strong legal interventions for privacy protection. The 18% Low we called the “Privacy Unconcerned,” basically focusing on consumer benefits and law-and-order values, without apprehensions about how their personal data is being used by organizations. The 57% Medium group we termed “Privacy Pragmatists,” looking in each situation to see whether information collected is really needed or a legitimate social function and whether safeguards of fair information practices are being followed by businesses and government.

- **Consumer Privacy Concern**

Focusing specifically on issues such as consumer credit, insurance, employment, and direct marketing, a 1991 Harris/Equifax survey developed a Consumer Privacy Concern Index that showed the public to divide in this area into 46% High Concern; 36% Moderate Concern, and 17% Low Concern. This documented the fact that media attention to consumer privacy issues and major expansions in the handling of consumer information in computerized databases had produced a Consumer Privacy Concern High significantly larger than the High for General Privacy Concern (45% compared to 25%).

- **Medical Privacy Concern**

With these two prior indexes for comparison, we set out in 1993 to find out how many Americans would score as High in medical privacy concern. We used three measures:

- respondents who themselves or a family member have used mental health services (22%);
- respondents who report that their personal medical information was disclosed improperly (27%); and
- respondents who scored High on our Medical Sensitivity Index (see above), which was based on two questions measuring computer fear and two measuring concern over circulation of medical information (13%).

Each of these measures, as we have already discussed, produced strong correlation between these respondents and strong privacy-oriented positions on a majority of our 39-question data set. After eliminating duplications among the three sets of respondents, we found that 48% of the public — representing 89 million Americans — fall into the High Concern position on issues of medical privacy, slightly higher even than for consumer privacy.

As a baseline for considering medical privacy issues in the handling of medical records, the development of health information systems and the formulation of national health care reform, policy makers should see almost half of the American public approaching such issues from a High Medical Privacy Concern.

Public and Leaders Compared

The Leaders sample of 651 persons was divided into three groups and nine sub-groups: (1) leaders from health services (hospital, HMO, and health insurance senior executives; physicians; nurses; and medical society executives); (2) government officials (state and federal legislators and regulatory officials concerned with health affairs); and (3) employers (represented by senior human resources executives).

Among these leader groups, physicians adopted a strong privacy position more often than the other leader categories in 14 of 24 key questions, and nurses higher in 10 of 24. Government officials as a group chose strong privacy positions somewhat more often than health services executives as a group.

However, unlike situations in other sectors where industry leaders surveyed register as significantly less concerned about privacy and privacy protection measures than the public, health services leaders and employers in the 1993 sample scored quite similarly in privacy attitudes to the public. Industry leaders were more privacy oriented than the public on nine questions; about the same in six; and the public was more privacy-oriented in nine questions. For example:

Leaders More Privacy Oriented Than the Public

	Public	Leaders
Protecting medical record confidentiality absolutely essential in health care reform	36%	43%
Very concerned that medical claims information may be seen by employer	22%	28%
Not acceptable for employers to see which employees are heavy users of health benefit.....	48%	51%
Very important that information-processing organizations have strong privacy policies	54%	76%
Favor federal legislation protecting medical confidentiality in national health care reform	56%	58%

Public More Privacy Oriented Than Leaders

Computer use often gives medical information to people who shouldn't see it	64 %	43%
Worried about computer use in health care reform	70%	64%
Concerned about a health identification number	57%	30%
Extremely important to create national medical privacy board	46%	28%

Overall, the public is higher than the leaders in medical sensitivity, computer fears, and favoring strong regulation, while the leaders are higher in controlling misuses of sensitive medical information and favoring strong privacy policies set by organizations handling medical information.

Leaders are also more pessimistic about protection of privacy in health care reform than the public is. While 54% of the public feels that privacy of medical records will probably be better protected in health care reform than it is today, only 23% of leaders think that will probably happen. And, in a question asked only of the leaders, a bare 50% said that they felt increased computerization of medical and health records "could be managed to help strengthen the confidentiality of such records," while 45% felt computerization "is almost certain to weaken confidentiality." (Five percent had no opinion.)

Implications for Health Care Reform and Health Information Systems

Though the public shows strong support for health care reform and is more optimistic than pessimistic about the possibilities for protecting medical confidentiality in a new national system, a number of trends suggest there will be significant problems in convincing the public that medical and health privacy is really being adequately assured in national health care reform.

Five indicators from past Harris surveys, updated in 1993, document the troubled mood from which the public will approach privacy issues in health care reform in the mid-90's:

	Public Concern			
	1978	1990	1992	1993
High and medium distrust in institutions	49%	55%	-	75%
Concern about threats to personal privacy	64%	79%	79%	80%
Believe consumers have lost all control over circulation of their personal information	-	71%	76%	80%
Believe technology almost out of control	43%	45%	-	50%
Believe computers must be sharply restricted if privacy is to be preserved	63%	-	67%	71%

What these high public scores on distrust of institutions, privacy concerns, and fear of computer abuses indicate is that it will take very strong and concrete actions by health providers, health care support organizations, health information processing organizations, public health agencies, Congress, and the Clinton Administration to convince a skeptical public that enough is being done to safeguard medical privacy rights. The fact that there is agreement between the public and all of the leader groups that comprehensive federal legislation is needed to protect medical confidentiality in any national health care reform provides a promising foundation for that effort. It is also quite promising that leaders and the public seem to agree on what should be the major components of such legislation, though there will obviously be difficult issues to resolve in balancing privacy interests with

administrative-disclosure needs and larger societal interests.

Beyond health care reform, the public concerns in the previous chart represent a strong signal to all organizations handling personal medical information that serious, detailed and effective attention must be paid to assuring privacy, confidentiality, and security in the handling of health information. This will be especially necessary as the nation's health system — with or without official health care reform — moves into more computerization of medical records and transactions, use of identification and “smart” cards, greater electronic exchanges of medical information, and reliance on various community and regional associations and specialized data-processing organizations to coordinate health-services administration and cost controls.

The public clearly wants an information-trusteeship ethos to pervade all of these settings where increasingly detailed and sensitive individual health information is being collected, stored, and transmitted.

CHAPTER 1: Personal Privacy In America Today

Public Concern About Threats To Privacy

The American public continues to be deeply concerned about threats to personal privacy. However, the upward climb of this concern, first measured in 1978*, has remained relatively stable since 1983. Eight of 10 Americans are "very" or "somewhat concerned" about threats to their personal privacy (80%), which is almost the same percentage of adults in the 1990** Equifax study. The number of people who are *very concerned* continues to grow (from 46% in 1990 to 49% in this current study).

Among racial and ethnic groups, Blacks and Hispanics express a higher degree of concern, paralleling results of three years ago. Other groups that show a great deal of concern are women (86%), adults aged 30-39 (85%), and those who describe their political philosophy as being liberal (86%). Among those with less than a high school education, fully 55% are very concerned, compared to 49% of the public and only 46% of college graduates and post graduates. In general, people with the lowest level of education and highest level of education differ by a 9% spread. The same is true with income, with a 10% spread in the "very concerned" between those earning the highest level of income and those earning the lowest. (TABLE 1-1)

Leadership Concern About Threats To Privacy

Leaders (78%) mirror the public when it comes to concerns about personal privacy being threatened. Physicians and heads of medical societies, health insurers and hospital CEOs express the greatest concern, ranging from 83% to 86%. In contrast, only 62% of CEOs of HMOs express concern. While just over two-thirds of congressional aides (68%), answering as proxies for federally elected representatives, say they are concerned about threats to personal privacy, they are not worried as much as their constituents (80%)³.

It is interesting to note that physicians feel "very concerned" to a higher degree (50%) than any of the other leadership groups. They are the first leadership group surveyed (in this study and the 1990 study) to express a level of concern similar to the "very concerned" public (49%). Human resources executives, the only leader group interviewed both in 1990 and 1993, have become a great deal more concerned about personal privacy (up from 69% three years ago to 80% now). (TABLE 1-2)

*Dimensions Of Privacy. Harris, 1979.

** *The Equifax Report On Consumers In The Information Age*. Louis Harris and Associates, Inc., 1990.

³When 49.3 very concerned and 30.3 somewhat concerned are added together, and rules of rounding applied, the total of the two responses is actually 80%.

Q.X1

TABLE 1-1
PUBLIC CONCERN ABOUT THREATS TO PERSONAL PRIVACY

Q.: How concerned are you about threats to your personal privacy in America today — very concerned, somewhat concerned, not very concerned or not at all concerned?

	Base	Very Concerned	Somewhat Concerned	Not Very Concerned	Not At All Concerned	Not Sure
Total	1000 %	49	30	11	6	3
Total (1990)*	2254 %	46	33	14	6	1
Gender						
Male	474 %	44	30	14	8	5
Female	526 %	55	31	9	4	1
Age						
18-24	123 %	43	36	16	4	—
25-29	115 %	45	35	10	9	1
30-39	229 %	47	38	10	4	1
40-49	204 %	51	26	10	9	4
50-64	180 %	56	23	10	5	5
65 and older	145 %	51	24	14	6	5
Education						
Less than high school	79 %	55	25	8	5	8
High school	336 %	48	31	10	9	2
Some college	274 %	50	31	13	5	1
College graduate	202 %	46	33	16	4	1
Post graduate	107 %	46	32	14	6	2
Race/Ethnicity						
White	857 %	46	32	12	6	3
Black	94 %	69	17	6	7	—
Hispanic	45 %	62	23	7	3	4
Political Philosophy						
Conservative	405 %	51	27	12	6	4
Moderate	392 %	48	32	14	6	1
Liberal	176 %	52	34	5	7	1
Income						
\$15,000 or less	184 %	42	34	13	5	6
\$15,001-\$35,000	357 %	54	28	10	6	2
\$35,001-\$50,000	161 %	42	33	11	11	2
\$50,001-\$75,000	130 %	50	29	16	5	—
\$75,001 & over	96 %	52	32	10	5	1

* *The Equifax Report On Consumers In The Information Age*. Louis Harris and Associates, Inc., 1990

General Statements About Business And Government

Three years ago Americans were asked specific statements about business and government in order to create a "distrust index" which was found to correlate strongly with attitudes about privacy (the stronger the level of distrust, the more concern about privacy). Since 1990, the public has developed even stronger, negative views. This increased level of distrust shows in their responses to the following statements:

- Technology has almost gotten out of control. (Half of Americans agree, an increase of 5% from 1990.)
- Government can generally be trusted to look after our interests. (75% disagree with this statement, up from 64% in 1990.)
- The way one votes has no effect on what the government does. (Slightly more Americans now agree; 42% compared to 38% in 1990.)
- In general, business helps us more than it harms us. (27% of the public now disagrees with this statement, compared to the 21% in 1990.)

Leaders' views on the same four statements are not quite as negative:

- Technology has almost gotten out of control. (26% of the leaders agree, 24 percentage points lower than the public.)
- Government can generally be trusted to look after our interests. (70% of leaders disagree with this statement, close to the level of skepticism reported by 75% of the public.)
- The way one votes has no effect on what the government does. (Leaders agree with this statement to a lesser degree than the public, 28% to 42%.)
- In general, business helps us more than it harms us. (11% of leaders disagree, compared to 27% of the public.)

Leaders have more faith than the public in the role of business, in the power of their vote, and have less fear of technology than the public. They do, however, share the public's concerns about whether the government looks after their interests. (TABLE 1-3)

Q.X1

TABLE 1-2
LEADERS' CONCERN ABOUT THREATS TO PERSONAL PRIVACY

Q.: How concerned are you about threats to your personal privacy in America today — very concerned, somewhat concerned, not very concerned or not at all concerned?

	Base	Very Concerned	Somewhat Concerned	Not Very Concerned	Not At All Concerned	Not Sure
Total Leaders	651 %	33	45	17	5	*
Total Public	1000 %	49	30	11	6	3
Hospital CEOs	101 %	35	48	13	5	—
HMO CEOs	50 %	18	44	28	10	—
Health Insurer CEOs	31 %	32	52	10	6	—
Physicians	100 %	34	42	18	6	—
Nurses	50 %	34	42	18	6	—
Medical Society Heads	50 %	26	60	10	4	—
State Regulators	30 %	27	53	17	—	3
State Legislators	68 %	43	31	22	4	—
Congressional Aides	70 %	31	37	24	7	—
Human Resources Executives 1993	101 %	22	58	18	2	—
	Base	Very Concerned	Somewhat Concerned	Not Very Concerned	Not At All Concerned	Not Sure
Human Resources Executives 1993	101 %	22	58	18	2	—
Human Resources Executives 1990**	203 %	18	51	26	5	—

*Less than 0.5%.

** *The Equifax Report On Consumers In The Information Age*. Louis Harris and Associates, Inc., 1990.

TABLE 1-3
AGREEMENT OR DISAGREEMENT WITH CERTAIN STATEMENTS ABOUT BUSINESS, TECHNOLOGY AND GOVERNMENT

Q.: For each of the following statements, please tell me whether you tend to agree or disagree?

	1990**																				
	1993				Leaders (Base: 651)				Public (Base: 2,254)				Leaders (Base: 916)								
	Public (Base: 1,000)		Not Sure %		Disagree %		Agree %		Disagree %		Agree %		Disagree %		Agree %		Disagree %		Agree %		Not Sure %
In general, business helps us more than it harms us	69	27	4	87	11	2	76	21	1	2	94	5	•	1							
Technology has almost gotten out of control	50	47	3	26	73	1	45	53	1	1	12	88	•	•							
The way one votes has no effect on what the government does	42	57	2	28	71	1	38	61	1	1	19	80	1	•							
Government can generally be trusted to look after our interests	23	75	2	29	70	2	35	64	•	1	37	62	1	1							

*Less than 0.5%.

**The Equifax Report On Consumers In The Information Age. Louis Harris and Associates, Inc., 1990.

The Distrust Index — Public and Leaders

The distrust index, developed in 1990, combines the levels of distrust toward (1) business (2) technology with the levels of distrust over (3) voting (4) government to create a four-factor index as follows:

“Agree” responses to items 2 and 3 or “disagree” responses to items 1 and 4 were considered distrustful answers. Respondents were then placed into one of four categories.

- Those respondents who gave distrustful responses on 3 or 4 items were considered to be highly distrustful.
- Those who gave distrustful responses on 2 of 4 items were considered to be moderately distrustful.
- Those who gave distrustful responses on only 1 of 4 items were considered to have a low level of distrust.
- Those who did not give a distrustful response on any of the 4 items were considered to be not distrustful.

The findings show that 32% of the public, or approximately 56 million Americans, (an increase of 9% from 1990), are highly distrustful. The percentage of those who are considered moderately distrustful (31%) has remained stable since 1990 (32%). Eight percent are now considered to be not distrustful at all, a drop of 6 percentage points in only three years.

The distrust index produced for the leadership demonstrates clearly that leaders are more trusting than the public.

According to the distrust index, 12% of leaders can be categorized as highly distrustful, which is a third of the percentage for the public on the same measure. The percentages of leaders (29%) and the public (31%) considered to be moderately distrustful is very similar. The remainder of the leaders fall into the “low distrustful” category, with 20% being “not at all distrustful.” (TABLE 1-4)

**TABLE 1-4
DISTRUST INDEX**

	Total Leaders	Total Public
Base:	651	1000
	%	%
Distrust Index		
High	12	32
Moderate	29	31
Low	39	29
None	20	8

Concern About Threats To Personal Privacy Correlated With Distrust Index

Americans considered to be highly distrustful are extremely worried about threats to their personal privacy (84% are "very" or "somewhat concerned"). Even a majority (69%) of those with no distrust at all are very or somewhat concerned about personal privacy. This is, however, a slight dip from the 67% of those with no distrust at all who were concerned about privacy threats in 1990.

Like the public, leaders who are highly distrustful overwhelmingly express concern about threats to their personal privacy (86%). More than three-fourths (83%) of the leaders categorized as moderately distrustful say they are very or somewhat concerned. Seventy-three percent of leaders with a low distrust index are concerned, and the leaders designated as "not at all distrustful" are only slightly greater in their level of concern (71%) than the same segment in the public study (69%). (For a discussion of the linkage between distrust levels and attitudes toward health information privacy issues, see Dr. Westin's opening essay in this report.) (TABLE 1-5)

General Statements About Privacy And Computers

A series of statements were presented to Americans to measure the extent of their attitudes on the issues of privacy and computers. The public is concerned about various types of organizations maintaining personal information on computers and wants controls to be put in place:

- Only 4 of 10 Americans say their "rights to privacy are adequately protected today by laws and organizational practices," and only 9% agree strongly with this statement.
- When it comes to the consumer's loss of "all control over how personal information about them is circulated and *used by companies*," 80% of the public feels this way. This reflects a rise of 9% from 1991* and 1990 when 71% agreed with this statement. However, 76% agreed with this statement in 1992**. Four percent disagree strongly with that statement.
- Asked if "computers have improved the quality of life in the society," 76% of adults answer "yes," down slightly from 79% in 1992.
- However, 71% feel "if privacy is to be preserved, the use of computers must be sharply restricted in the future." In 1992, this figure was 67%, indicating a slight increase on this measure. (TABLES 1-6 and 1-7)

* *Harris-Equisfax Consumer Privacy Survey* Louis Harris and Associates, Inc., 1991.

** *Harris-Equisfax Consumer Privacy Survey* Louis Harris and Associates, Inc., 1992.

*QXI

TABLE 1-5
 EXTENT PUBLIC IS CONCERNED ABOUT THREATS TO PERSONAL PRIVACY CORRELATED WITH
 1993, 1990, AND 1978 DISTRUST INDEX

Q.: How concerned are you about threats to your personal privacy in America today — very concerned, somewhat concerned, not very concerned or not at all concerned?

	Distrust Index 1993				Distrust Index 1990**				Distrust Index 1978***							
	Total Public	High %	Mode-rate %	Low %	Total Public %	High %	Mode-rate %	Low %	Total Public %	High %	Mode-rate %	Low %	Total Public %	High %	Mode-rate %	Low %
Base	1000	297	311	303	89	2254	488	669	740	357	1511	315	424	511	261	
	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Very concerned	49	60	48	45	32	46	55	50	42	29	31	47	30	27	21	
Somewhat concerned	30	24	35	30	37	33	30	32	35	38	33	30	32	33	35	
Not very concerned	11	8	10	14	24	14	8	12	17	22	17	11	20	19	17	
Not at all concerned	6	6	5	9	3	6	6	5	5	10	19	12	17	21	26	
Not sure	3	3	2	3	4	1	*	1	1	1	1	*	*	1	1	

*Less than 0.5%.

The Equifax Report On Consumers In The Information Age*. Louis Harris and Associates, Inc., 1990.*Dimensions Of Privacy*. Harris, 1979.

Q.X3

TABLE 1-6
PUBLIC AGREEMENT OR DISAGREEMENT WITH
CERTAIN STATEMENTS CONCERNING PRIVACY

Q.: Consumers have lost all control over how personal information about them is circulated and used by companies.

	1993	1992*	1991**	1990***
Base:	1,000	1,254	1,255	2,254
	%	%	%	%
Agree strongly	47	47	37	71
Agree somewhat	33	29	34	
Disagree somewhat	15	13	20	27
Disagree strongly	4	7	3	
Not sure	2	3	4	3

Q.: If privacy is to be preserved, the use of computers must be sharply restricted in the future.

	1993	1992*
Base:	1,000	1,254
	%	%
Agree strongly	40	39
Agree somewhat	31	28
Disagree somewhat	17	18
Disagree strongly	10	11
Not sure	2	4

NOTE: This question was not asked in 1991 and 1990.

* *Harris-Equifax Consumer Privacy Survey* Louis Harris and Associates, Inc., 1992.

** *Harris-Equifax Consumer Privacy Survey* Louis Harris and Associates, Inc., 1991.

*** *The Equifax Report On Consumers In The Information Age*. Louis Harris and Associates, Inc., 1990.
 Question asked "agree" or "disagree" in 1990.

Q.X3

TABLE 1-6 (Continued)
PUBLIC AGREEMENT OR DISAGREEMENT WITH
CERTAIN STATEMENTS CONCERNING PRIVACY

Q.: Computers have improved the quality of life in our society.

	1993	1992*
Base:	1,000	1,254
	%	%
Agree strongly	36	45
Agree somewhat	40	34
Disagree somewhat	13	10
Disagree strongly	10	8
Not sure	1	2

NOTE: This question was not asked in 1991 and 1990.

Q.: My rights to privacy are adequately protected today by laws and organizational practices.

	1993
Base:	1,000
	%
Agree strongly	9
Agree somewhat	31
Disagree somewhat	29
Disagree strongly	29
Not sure	2

NOTE: This question was not asked in 1992, 1991, and 1990.

*Harris-Equifax Consumer Privacy Survey Louis Harris and Associates, Inc., 1992.

Attitudes As A Function Of Age

Age largely determines attitudes toward two issues about computer usage. Of adults aged 18-29, 30-49 and 50 and over, the percentages who strongly agree that "computers have improved the quality of life" fall off sharply: 45%, 39% and 27%, respectively. The reverse is true when asked about restricting computer use; the older the respondents, the more they favor sharp restrictions. Just over half (52%) of adults 50 and over strongly agree that "the use of computers must be sharply restricted," compared to 38% of those aged 30-49 and only 27% of Americans 18-29. (TABLE 1-7 and 1-8)

Q.X3-4

TABLE 1-7
EXTENT TO WHICH PUBLIC AGREES THAT FUTURE USE OF
COMPUTERS MUST BE RESTRICTED TO PRESERVE PRIVACY

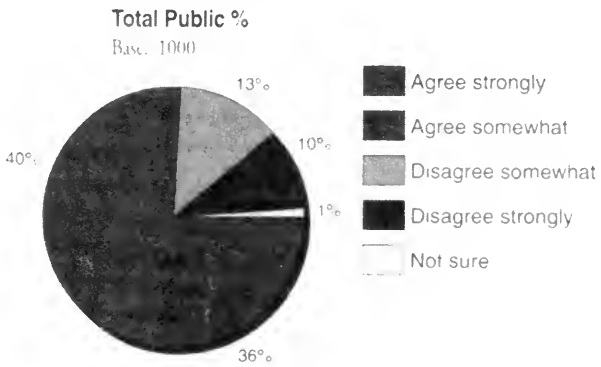
Q: If privacy is to be preserved, the use of computers must be sharply restricted in the future — do you agree strongly, agree somewhat, disagree somewhat or disagree strongly?

	Total	Age		
		18-29	30-49	50 & Older
Base:	1000	238	433	325
	%	%	%	%
Agree strongly	40	27	38	52
Agree somewhat	31	38	32	25
Disagree somewhat	17	21	17	15
Disagree strongly	10	13	12	5
Not sure	2	1	1	3

Q.X3-3

TABLE 1-8
EXTENT TO WHICH PUBLIC AGREES THAT COMPUTERS
HAVE IMPROVED THE QUALITY OF LIFE

Q.: Computers have improved the quality of life in our society — do you agree strongly, agree somewhat, disagree somewhat, or disagree strongly?



CHAPTER 2: Attitudes and Experiences of the American Public with Health Care and Medical Records

Health Rating And Do They Visit Clinic Or Doctor

Most adults in the U.S. report that they are healthy. A large majority (84%) state their health is either "excellent" (36%) or "pretty good" (48%). Only 3% rated their health as being "poor," while 13% answered that their health was only "fair." (TABLE 2-1)

Q.A1

**TABLE 2-1
HEALTH (PUBLIC)**

Q.: Overall would you say your health is excellent, pretty good, fair, or poor?

	Total	Gender		Age					65 & Older
		Male	Female	18-24	25-29	30-39	40-49	50-64	
Base	1000	474	526	123	115	229	2204	180	145
	%	%	%	%	%	%	%	%	%
Excellent	36	36	37	40	48	43	42	29	18
Pretty good	48	49	47	47	43	44	47	49	54
Fair	13	11	14	13	8	12	9	17	18
Poor	3	4	2	-	1	1	1	4	10
Not sure	*	*	-	-	-	-	*	*	-

*Less than 0.5%.

Differences Among Those Who Visit A Clinic Or Doctor

Most Americans (just over 3 of 4 adults or 138 million people) say there is "a particular clinic, health center, doctor's office or some other place where [they] go when [they] are sick or need advice about [their] health."

However, there are several interesting differences between segments of the population. Hispanics are more likely not to have a regular source of care than Whites or Blacks. Among the uninsured, less than half (more than 11 million people) say they have a regular source of care (48%). Women are 10 percentage points higher than men in reporting they do have a regular source of care. (TABLE 2-2)

Q.B1

TABLE 2-2
WHETHER PUBLIC HAS A PARTICULAR PLACE TO
GO WHEN SICK OR NEEDS ADVICE ABOUT HEALTH

Q.: Is there a particular clinic, health center, doctor's office or some other place where you go when you are sick or need advice about your health?

	Gender			Education				
	Total	Male	Female	Less Than High School	High School	Some College	College Graduate	Post Graduate
Base	1000	474	526	79	336	274	202	107
	%	%	%	%	%	%	%	%
Yes	76	71	81	70	77	78	79	83
No	24	28	19	30	23	22	21	17
Not Sure	*	*	*	-	*	*	-	-

	Race/Ethnicity				Income					
	Total	White	Black	Hispanic	\$15,000 or Less	\$15,001 to \$35,000	\$35,001 to \$50,000	\$50,001 to \$75,000	\$75,001 to Over	Uninsured
Base	1000	857	94	45	184	357	161	130	96	114
	%	%	%	%	%	%	%	%	%	%
Yes	76	76	86	60	69	78	79	88	72	48
No	24	24	13	40	31	22	21	12	28	52
Not Sure	*	*	1	-	-	-	-	1	-	-

*Less than 0.5%.

How Much Do They Know About Their Records

Most Americans believe they know something, if not everything, about the contents of their medical records.

Very nearly nine-tenths of all adults (87%) say they "know everything" or "have a general idea, but don't know in detail" about the information in their medical records. However, 13% (18 million Americans) say they "don't know anything" about the information in the medical records that are kept in the place they regularly visit for treatment.

Adults who have attained a higher level of education and adults who are older say, in larger numbers, that they know everything or at least have a general knowledge about the information in their medical records. (TABLE 2-3)

Q.B2

TABLE 2-3
HOW MUCH IS KNOWN ABOUT THE CONTENTS OF
AN INDIVIDUAL'S MEDICAL RECORD

Q: How much do you know about the information that is in your medical record in that place? Would you say you know everything that is in it, or that you have a general idea but don't know in detail, or that you don't know anything about your records?

Base: Has a particular place to go when sick or needs advice about health

	Total	Education				
		Less Than High School	High School	Some College	College Graduate	Post Graduate
Base	781	55	257	217	162	89
	%	%	%	%	%	
Know everything	25	23	24	25	29	30
Have a general idea but don't know in detail	62	54	65	66	61	64
Don't know anything	13	23	11	9	9	6
Not sure	*	-	-	-	1	-

*Less than 0.5%.

Q.B2

TABLE 2-3 (Continued)
HOW MUCH IS KNOWN ABOUT THE CONTENTS OF
AN INDIVIDUAL'S MEDICAL RECORD

Q.: How much do you know about the information that is in your medical record in that place?
 Would you say you know everything that is in it, or that you have a general idea but don't know in detail, or that you don't know anything about your records?

Base: Has a particular place to go when sick or needs advice about health

	Total	Race/Ethnicity			Age					65 & Older
		White	Black	Hispanic	18-24	25-29	30-39	40-49	50-64	
Base	781	669	80	28	82	77	181	167	148	122
	%	%	%	%	%	%	%	%	%	%
Know everything	25	26	19	19	27	31	23	24	18	32
Have a general idea but don't know in detail	62	61	70	65	56	58	64	63	69	58
Don't know anything	13	13	11	16	17	11	14	12	13	9
Not sure	*	*	-	-	-	-	-	-	-	1

*Less than 0.5%.

Have They Asked For Records

While most people have not done so, nearly one of every four Americans (24%) (representing 34 million adults) who have a particular place to go when sick or in need of advice about health, have asked their health care provider for their complete records at some time. (TABLE 2-4)

Q.B3

TABLE 2-4
WHETHER ASKED TO SEE THEIR MEDICAL RECORD (PUBLIC)

Q.: Have you ever asked your health care provider to show you your complete medical record, or not?

Base: Has a particular place to go when sick or needs advice about health

	Total
Base	781
	%
Yes	24
No	76
Not sure	*

Why Did They Ask For Records

In most cases, "curiosity" was the reason given for asking to see the records (44%). The next three reasons given most often were:

- the need to transfer records, changed doctors or moved (18%).
- the need to see results of tests/treatments (13%).
- wanting to check medical records for accuracy (9%). (TABLE 2-5)

*Less than 0.5%.

Q.B4

TABLE 2-5
REASON FOR ASKING TO SEE THEIR RECORD (PUBLIC)

Q.: What was your reason for asking to see your record?

Base: Has a particular place to go when sick or needs advice about health and asked health care provider to see complete medical record

	Total
Base	199
	%
Curiosity	44
Need to transfer records: changed doctors/moved	18
Need to see results of tests/treatment	13
To check for accuracy	9
I'm a medical professional: doctor/nurse	2
Wanted a copy for personal records	2
All others	6
Don't know	6

Was The Record Shown And Why Did They Not Get Record

The great majority of Americans who requested to see their medical records (92%) had their requests granted. However, 8% were not given access to their medical records kept by a health care professional. The reason given most often by the provider in refusing the request was that the records couldn't be located (31%). Of the people who asked for and didn't receive a copy of their records, 25%, or 4 million, were given no reason and simply had the request denied. (TABLE 2-6 and 2-7)

Q.B5

TABLE 2-6
WHETHER THEIR MEDICAL RECORD WAS INSPECTED (PUBLIC)

Q.: Was your complete record shown to you or a copy of it given to you?

Base: Has a particular place to go when sick or needs advice about health and asked health care provider to see complete medical record

	Total
Base	199
	%
Yes	92
No	8
Not sure	-

Q.B7

TABLE 2-7
REASON GIVEN FOR REFUSING TO PROVIDE MEDICAL RECORD (PUBLIC)

Q.: What was the reason given for refusing to provide it to you?

Base: Complete medical record was not shown (as requested).

	Total Public
Base:	18 %
Couldn't locate	31
Gave no reason/just refused	25
All others	25
Don't know	18

Did They Understand Record

Respondents who were given a copy of their records were almost unanimous (97%) in saying they understood them or had them explained in a satisfactory manner. (TABLE 2-8)

Q.B6

TABLE 2-8
WHETHER THEIR MEDICAL RECORD WAS UNDERSTOOD (PUBLIC)

Q.: Did you understand it, or have it explained to you in a satisfactory way, or not?

Base: Has a particular place to go when sick or needs advice about health, asked health provider to see complete medical record, and complete medical record was shown

	Total
Base	181 %
Yes	97
No	3
Not sure	*

*Less than 0.5%.

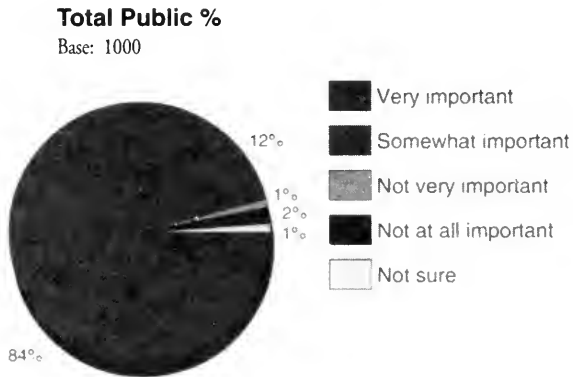
How Important Is The Legal Right To Obtain Record

The legal right to obtain a copy of one's medical records is important to the American public. When asked how important this right is, 96% of all people surveyed say it is very or somewhat important, with 84% saying "very important." (TABLE 2-9)

Q.B8

TABLE 2-9
IMPORTANCE OF HAVING THE LEGAL RIGHT TO OBTAIN A COPY
OF AN INDIVIDUAL'S MEDICAL RECORD (PUBLIC)

Q.: How important do you think it is that you should have the legal right to obtain a copy of your medical records — very important, somewhat important, not very important, or not important at all?



CHAPTER 3: Uses of Medical Information for Marketing and Research

For Marketing And Fund Raising

Most people are opposed to the use of their medical information without their permission for direct mail about new medication or for hospital fund raising. Fully 60% say it would be unacceptable to use their medical records for direct mail by pharmaceutical companies, and an even larger 66% say it would be unacceptable for hospitals to use patient records to solicit donations.

Across age groups, there is a steady rise in those people who say such direct mail by drug companies is "not very acceptable" or "not at all acceptable," peaking with the 50-64 year olds (72%) then declining slightly with those 65 or older (65%). More educated Americans also find this practice unacceptable.

Only a third (33%) say it is at least somewhat acceptable for hospital fund raisers to use patient names and addresses in soliciting donations without prior approval. Two-thirds of adults do not believe this practice is acceptable and nearly half of the adult population find this situation not at all acceptable.

Slightly more than three-fourths (77%) of the people with post graduate degrees find this practice "not very acceptable" or "not at all acceptable." Paralleling the results described above, people who are 50-64 years old are also the most likely to find it unacceptable to use medical information for fund raising (77%). (TABLES 3-1 and 3-2)

Q.G1-1

**TABLE 3-1
HOW ACCEPTABLE IT IS TO USE CERTAIN MEDICAL INFORMATION (PHARMACIST) ABOUT
INDIVIDUALS WITHOUT OBTAINING THEIR PRIOR APPROVAL (PUBLIC)**

Q.: In the following situations, how acceptable do you think it is to use medical information about individuals without first obtaining approval from the individual? Pharmacists providing the names and addresses of customers using certain medications to companies that want to mail out information about or make offers of new medications for those conditions. Would this be very acceptable, somewhat acceptable, not very acceptable, not at all acceptable?

	Age										Education					Race/Ethnicity		
	18-24	25-29	30-39	40-49	50-64	65 & Older	Less Than High School	High School	Some College	College Graduate	Post-Graduate	White	Black	Hispanic				
Total	11	11	8	14	12	9	19	12	8	4	4	857	94	45				
%	11	11	8	14	12	9	19	12	8	4	4	10	18	16				
Base:	1000	123	115	229	204	180	145	336	274	202	107	857	94	45				
	11	11	8	14	12	9	19	12	8	4	4	10	18	16				
Very acceptable	28	45	33	34	23	15	25	33	33	22	18	27	31	33				
Somewhat acceptable	19	15	24	20	14	23	18	14	19	27	25	20	9	22				
Not very acceptable	41	28	32	38	49	46	38	40	40	45	52	42	42	28				
Nor at all acceptable	1	-	-	1	2	2	-	1	-	1	1	1	-	1				
Nor sure																		

*Less than 0.5%.

Q.G1-2

TABLE 3-2
HOW ACCEPTABLE IT IS TO USE CERTAIN MEDICAL INFORMATION (FUND RAISING) ABOUT
INDIVIDUALS WITHOUT OBTAINING THEIR PRIOR APPROVAL (PUBLIC)

Q.: In the following situations, how acceptable do you think it is to use medical information about individuals without first obtaining approval from the individual? Hospital fundraisers getting the names of those who have been patients at the hospital to write to them for donations to the hospital. Would this be very acceptable, somewhat acceptable, not very acceptable, not at all acceptable?

	Age										Education						Race/Ethnicity		
	18-24	25-29	30-39	40-49	50-64	65 & Older	Less Than High School	High School	Some College	College Graduate	Post-Graduate	White	Black	Hispanic					
Base:	123	115	229	204	180	145	79	336	274	202	107	857	94	45					
	%	%	%	%	%	%	%	%	%	%	%	%	%	%					
Very acceptable	9	6	5	8	6	6	12	7	4	2	4	5	14	9					
Somewhat acceptable	35	37	30	22	15	31	34	25	27	28	19	26	29	41					
Not very acceptable	24	25	20	18	20	13	15	19	21	22	21	20	17	21					
Not at all acceptable	31	32	45	52	57	51	38	49	47	47	56	48	40	27					
Not sure	1	-	1	-	2	-	1	-	*	1	-	1	-	3					

*Less than 0.5%.

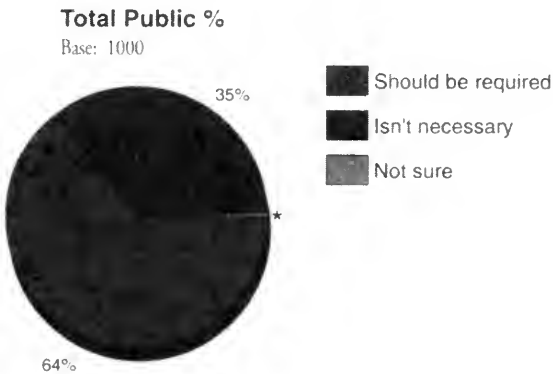
Should Permission Be Required For Medical Records To Be Used In Research And Should Permission Be Required Each Time

The concern of the public about having their medical records used without their approval is also evident when the subject is medical research. Even if not identified personally in any publication of the research, nearly two of three adults want to be asked for their permission. Well over half of those (56%) say permission to release information should be required each time a request is made. (TABLES 3-3 and 3-4)

Q.E1

**TABLE 3-3
WHETHER PERMISSION SHOULD BE REQUIRED
BEFORE MEDICAL RECORDS ARE USED FOR RESEARCH (PUBLIC)**

Q: Medical researchers sometimes need to use individual patient records to study the causes of diseases or the value of specific drugs or treatments. However, they do not release any information identifying specific patients. If you are not personally identified in any publication, should your permission be required before your medical records are used for research, or isn't that necessary?



Q.E2

TABLE 3-4
WHETHER PERMISSION SHOULD BE REQUIRED EACH TIME
BEFORE MEDICAL RECORDS ARE USED FOR RESEARCH (PUBLIC)

Q.: Should your permission be required each time a researcher seeks to use your medical records or would asking for general advance permission to use your records for medical research be sufficient?

Base: Permission should be required before medical records are used for research.

	Total
Base:	642
	%
Required each time	56
General permission is sufficient	42
Not sure	2

CHAPTER 4: Disclosure of Confidential Information and Medical Records

Leaders' Perceptions Of Public Concern About Threats To Medical Record's Confidentiality

A majority of the leaders believe that most Americans are either very concerned (28%) or somewhat concerned (43%) about threats to the confidentiality of their medical records.

The concern is perceived to the greatest degree by nurses (78%), state legislators (77%) and heads of medical societies (76%). Of all the leaders, human resource executives registered the lowest percentage (64%) in thinking the public is concerned about their medical records. (TABLE 4-1)

Q.M4

**TABLE 4-1
PERCEIVED LEVEL OF CONCERN ABOUT THREATS
TO MEDICAL RECORD'S CONFIDENTIALITY (LEADERS)**

Q.: How concerned do you think most Americans really are about threats to the confidentiality of their medical records — do you think they are very concerned, somewhat concerned, not very concerned or not at all concerned?

	Base		Very Concerned	Somewhat Concerned	Not Very Concerned	Not At All Concerned	Not Sure
Total Leaders	651	%	28	43	27	2	*
Hospital CEOs	101	%	23	46	30	2	-
HMO CEOs	50	%	20	50	26	4	-
Health Insurer CEO.	31	%	26	45	29	-	-
Physicians	100	%	29	39	29	2	1
Nurses	50	%	32	46	18	4	-
Medical Society Heads	50	%	30	46	24	-	-
State Regulators	30	%	30	40	30	-	-
State Legislators	68	%	49	28	21	3	-
Congressional Aides	70	%	31	43	24	1	-
Human Resources Executives	101	%	17	47	37	-	-

*Less than 0.5%.

Illness Of Self Or Family

Americans report that they or a member of their immediate family has experienced the following medical conditions or situations:

- 35% have had a serious illness such as a heart attack, stroke, or cancer.
- 22% have used the services of a psychologist, psychiatrist, or other mental-health professional.
- 19% have a long-term medical condition such as diabetes or epilepsy.
- 14% have a major physical or mental disability. (TABLE 4-2A)

Q.A2

TABLE 4-2A
SOME SPECIFIC MEDICAL EXPERIENCES (PUBLIC)

Q.: (Have/do) you or (has/does) a member of your immediate family (READ ITEM), or not?

	Yes %	No %	Not Sure %
Base: 1000			
Ever had a serious illness such as a heart attack, stroke, or cancer	35	65	1
Ever used the services of a psychologist, psychiatrist, or other mental-health professional	22	77	1
Have a long-term medical condition such as diabetes or epilepsy	19	80	1
Have any major physical or mental disabilities	14	85	1

Not Seeking Care Because Of Concern Over Job Prospects Or Other Life Opportunities

Seven percent of the public has wanted to seek services for a physical condition or mental health problem but didn't do so because they didn't want to harm their "job prospects or other life opportunities."⁶ People in the South (7%) or West (8%) are twice as likely as people in the East (3%) to respond affirmatively to this question. Mid-Westerners (11%), however, are almost four times as likely to respond this way than Easterners. People 65 years or older (2%) and those earning \$75,000 a year or more (2%) are much less likely to be constrained from seeking treatment by this concern than the rest of the public. (TABLE 4-2B)

⁶We asked these questions to test whether persons reporting such adverse medical conditions would have any different attitudes toward the confidentiality and privacy of medical records, or patient rights of access to them, than persons who did not report having such conditions. See Dr. Westin's essay for a discussion of these results.

Q.A2-5

TABLE 4-2B
WHETHER PUBLIC AVOIDED CARE BECAUSE OF
POTENTIAL HARM TO JOB OR OTHER OPPORTUNITIES

Q.: (Have/Do) you or (has/does) a member of your immediate family ... ever wanted to seek services for a physical condition or mental health problem but didn't do so because you didn't want to harm your job prospects or other life opportunities, or not?

	Base		Yes, Has	No, Has Not	Not Sure
Total	1000		7	92	1
Region					
East	238	%	3	97	1
Midwest	245	%	11	89	-
South	314	%	7	92	1
West	203	%	8	92	1
Gender					
Male	474	%	5	94	*
Female	526	%	9	90	1
Age					
18-24	123	%	8	90	2
25-29	115	%	8	92	-
30-39	229	%	9	91	-
40-49	204	%	7	92	1
50-64	180	%	9	90	1
65 and older	145	%	2	98	*
Income					
\$15,000 or less	184	%	9	91	-
\$15,001-\$35,000	357	%	8	92	1
\$35,001-\$50,000	161	%	7	92	1
\$50,001-\$75,000	130	%	7	92	2
\$75,001 & over	96	%	2	97	2

People Choosing Not To File An Insurance Claim

While a quarter of the public say they have, on occasion, chosen not to file insurance claims for medical bills, only a few (11% of these people) did so to protect their privacy or confidentiality. However, the 11% does represent 5 million people. Forty-eight percent of those who didn't file medical claims were evenly divided between those saying that the procedure was not covered and those who said that it was easier or eliminated paperwork. People with less than a high school education (36%), Blacks (33%), and Hispanics (37%) most frequently reported that the procedure not being covered was their reason for not filing a claim. People 65 years and older (40%) and college graduates (32%) lead the group that said the reason was that it was easier and eliminated paperwork. (TABLE 4-3)

*Less than 0.5%.

Q.H2B

TABLE 4-3
REASONS FOR NOT SUBMITTING MEDICAL CLAIMS (PUBLIC)

Q: Why was that?

Base: Respondent or immediate family member has paid for medical test, treatment, or counseling rather than submit a bill or claim under a health plan or program

	Education					Race/Ethnicity			Age					
	Total	Less Than High School	High School	Some College	College Graduate	Post Graduate	White	Black	Hispanic	18-24	25-29	30-39	40-49	50-64
Base	268	19	74	76	57	41	228	27	10	35	58	72	47	20
	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Procedure not covered	24	36	26	22	14	19	23	33	37	27	25	22	24	24
Eases/eliminates paperwork	24	15	25	23	32	26	25	21	25	12	20	25	26	23
Did not have insurance	13	13	14	16	11	5	13	8	12	16	17	15	12	11
Wanted confidentiality/privacy	11	15	7	9	11	13	10	20	-	15	19	13	7	10
Haven't met deductible	8	5	9	11	8	9	9	-	-	2	3	11	15	10
Minor bill/procedure	8	5	7	5	11	14	8	7	-	9	2	5	10	8
Needed quick medical attention	3	-	-	1	11	2	2	9	18	3	-	4	4	3
All others	4	-	2	4	6	13	5	-	-	8	4	3	5	3
Don't know	11	11	17	9	3	11	11	6	9	14	9	6	7	16

Have Professionals Disclosed Records

Many people and organizations obtain personal medical information about the public. Sizable minorities of the public (27%) report that such persons and organizations were guilty of improper disclosures. Health insurance companies were most often blamed for improper disclosure (15%), while pharmacies or druggists barely register a measurable amount (3%). In between, are clinics or hospitals (11%), public health agencies (10%), employers (9%) and doctors (7%). (TABLE 4-4).

Some specific findings of this question are:

- People with some college education (11%) and those with post graduate degrees (10%) are more likely to believe that a doctor has disclosed their medical information. This is more common among Blacks (11%), people who earn more than \$50,000 a year (12% in each of the higher income segments) and people between the ages of 40 and 49 (12%).
- On whether a hospital or clinic has ever disclosed medical records, people with more than a high school education (with a range of 14% - 16% across the three segments), Hispanics (23%), and people earning between \$50,001 and \$75,000 (21%) are the most likely to believe this is true.
- Health insurance companies were most frequently blamed by people for disclosing medical records information, particularly people with post graduate degrees (30%), those earning \$50,001 to \$75,000 (31%), and 40 - 49 year olds (20%). (TABLES 4-5 through 4-10)

Q.D1

TABLE 4-4
WHETHER PERSONAL MEDICAL INFORMATION WAS
EVER IMPROPERLY DISCLOSED (PUBLIC)

Q.: Do you believe that (READ EACH ITEM) has ever disclosed your personal medical information in a way that you felt was improper, or not?

	Yes	No	Not Sure
	%	%	%
Base: 1000			
Health insurance companies	15	82	3
A clinic or hospital that treated you or a family member	11	87	2
Public health agencies	10	86	4
Your employer or a family member's employer	9	89	1
A doctor who has treated you or a family member	7	92	1
A pharmacy or druggist who filled a prescription for you or a family member	3	95	1

Q.D1-1

TABLE 4-5
WHETHER PERSONAL MEDICAL INFORMATION WAS
EVER IMPROPERLY DISCLOSED (PUBLIC)

Q.: Do you believe that ... a doctor who has treated you or a family member ... has ever disclosed your personal medical information in a way that you felt was improper, or not?

	Base	%	Yes	No	Not Sure
Total	1000	%	7	92	1
Age					
18-24	123	%	10	89	1
25-29	115	%	8	92	-
30-39	229	%	7	93	1
40-49	204	%	12	86	2
50-64	180	%	6	92	1
65 and older	145	%	2	97	1
Education					
Less than high school	79	%	6	94	-
High school	336	%	6	93	1
Some college	274	%	11	88	1
College graduate	202	%	7	91	1
Post graduate	107	%	10	87	3
Race/Ethnicity					
White	857	%	7	92	1
Black	94	%	11	89	1
Hispanic	45	%	8	91	2
Income					
\$15,000 or less	184	%	7	93	1
\$15,001-\$35,000	357	%	7	93	1
\$35,001-\$50,000	161	%	6	93	2
\$50,001-\$75,000	130	%	12	87	1
\$75,001 & over	96	%	12	87	1

*Less than 0.5%

Q.D1-2

TABLE 4-6
WHETHER PERSONAL MEDICAL INFORMATION WAS
EVER IMPROPERLY DISCLOSED (PUBLIC)

Q.: Do you believe that ... a clinic or hospital that treated you or a family member ... has ever disclosed your personal medical information in a way that you felt was improper, or not?

	Base		Yes	No	Not Sure
Total	1000	%	11	87	2
Age					
18-24	123	%	14	86	1
25-29	115	%	11	88	1
30-39	229	%	12	87	*
40-49	204	%	14	84	2
50-64	180	%	14	83	3
65 and older	145	%	3	92	4
Education					
Less than high school	79	%	9	89	2
High school	336	%	9	90	1
Some college	274	%	15	84	2
College graduate	202	%	14	84	2
Post graduate	107	%	16	80	4
Race/Ethnicity					
White	857	%	11	88	2
Black	94	%	15	84	2
Hispanic	45	%	23	77	-
Income					
\$15,000 or less	184	%	10	90	-
\$15,001-\$35,000	357	%	11	87	2
\$35,001-\$50,000	161	%	9	89	2
\$50,001-\$75,000	130	%	21	77	2
\$75,001 & over	96	%	15	84	2

*Less than 0.5%.

Q:D1-3

TABLE 4-7
WHETHER PERSONAL MEDICAL INFORMATION WAS
EVER IMPROPERLY DISCLOSED (PUBLIC)

Q.: Do you believe that ... your employer or family member's employer ... has ever disclosed your personal medical information in a way that you felt was improper, or not?

	Base		Yes	No	Not Sure
Total	1000	%	9	89	1
Age					
18-24	123	%	13	86	1
25-29	115	%	12	88	-
30-39	229	%	11	88	1
40-49	204	%	10	89	1
50-64	180	%	6	92	2
65 and older	145	%	4	93	3
Education					
Less than high school	79	%	8	92	-
High school	336	%	8	91	1
Some college	274	%	10	87	2
College graduate	202	%	10	89	1
Post graduate	107	%	13	82	5
Race/Ethnicity					
White	857	%	9	90	1
Black	94	%	11	88	1
Hispanic	45	%	21	78	2
Income					
\$15,000 or less	184	%	8	90	1
\$15,001-\$35,000	357	%	9	91	1
\$35,001-\$50,000	161	%	12	87	1
\$50,001-\$75,000	130	%	11	87	2
\$75,001 & over	96	%	10	90	-

Q,D1-4

TABLE 4-8
WHETHER PERSONAL MEDICAL INFORMATION WAS
EVER IMPROPERLY DISCLOSED (PUBLIC)

Q.: Do you believe that ... a pharmacy or druggist who filled a prescription for you or a family member ... has ever disclosed your personal medical information in a way that you felt was improper, or not?

	Base		Yes	No	Not Sure
Total	1000	%	3	95	1
Age					
18-24	123	%	4	96	1
25-29	115	%	3	97	-
30-39	229	%	2	97	*
40-49	204	%	6	93	1
50-64	180	%	3	95	3
65 and older	145	%	2	94	4
Education					
Less than high school	79	%	3	97	-
High school	336	%	4	96	1
Some college	274	%	3	95	1
College graduate	202	%	3	94	3
Post graduate	107	%	4	92	3
Race/Ethnicity					
White	857	%	3	96	1
Black	94	%	4	95	1
Hispanic	45	%	5	95	-
Income					
\$15,000 or less	184	%	4	96	1
\$15,001-\$35,000	357	%	2	97	*
\$35,001-\$50,000	161	%	2	96	2
\$50,001-\$75,000	130	%	8	90	2
\$75,001 & over	96	%	4	96	1

*Less than 0.5%.

Q.D1-5

TABLE 4-9
WHETHER PERSONAL MEDICAL INFORMATION WAS
EVER IMPROPERLY DISCLOSED (PUBLIC)

Q.: Do you believe that ... health insurance companies ... have ever disclosed your personal medical information in a way that you felt was improper, or not?

	Base		Yes	No	Not Sure
Total	1000	%	15	82	3
Age					
18-24	123	%	12	87	1
25-29	115	%	11	89	1
30-39	229	%	16	83	1
40-49	204	%	20	75	5
50-64	180	%	17	79	4
65 and older	145	%	9	82	9
Education					
Less than high school	79	%	11	86	2
High school	336	%	12	85	3
Some college	274	%	16	79	5
College graduate	202	%	16	80	3
Post graduate	107	%	30	62	8
Race/Ethnicity					
White	857	%	14	82	4
Black	94	%	10	88	2
Hispanic	45	%	28	69	3
Income					
\$15,000 or less	184	%	9	88	3
\$15,001-\$35,000	357	%	12	84	4
\$35,001-\$50,000	161	%	14	84	2
\$50,001-\$75,000	130	%	31	68	2
\$75,001 & over	96	%	27	70	3

Q.D1-6

TABLE 4-10
WHETHER PERSONAL MEDICAL INFORMATION WAS
EVER IMPROPERLY DISCLOSED (PUBLIC)

Q.: Do you believe that ... public health agencies ... have ever disclosed your personal medical information in a way that you felt was improper, or not?

	Base		Yes	No	Not Sure
Total	1000	%	10	86	4
Age					
18-24	123	%	11	88	1
25-29	115	%	4	94	2
30-39	229	%	9	89	2
40-49	204	%	11	82	7
50-64	180	%	13	83	4
65 and older	145	%	10	84	7
Education					
Less than high school	79	%	12	85	3
High school	336	%	7	91	2
Some college	274	%	10	87	4
College graduate	202	%	12	82	6
Post graduate	107	%	16	77	6
Race/Ethnicity					
White	857	%	10	87	3
Black	94	%	12	84	4
Hispanic	45	%	20	76	4
Income					
\$15,000 or less	184	%	7	90	3
\$15,001-\$35,000	357	%	8	87	4
\$35,001-\$50,000	161	%	8	89	3
\$50,001-\$75,000	130	%	18	78	4
\$75,001 & over	96	%	18	80	2

Were They Embarrassed Or Harmed By Disclosure

Those adults who believe that an improper disclosure was made by an organization or individual were asked if they felt "that you or the family member were embarrassed or harmed by that disclosure." Just under one-third of this group said they did experience embarrassment or harm. This conviction is expressed to the same extent across all demographic groups, with one exception: only 15% of the most affluent respondents (those with a household income of \$75,001 and over) say they were embarrassed or harmed by the disclosure.

(TABLE 4-11)

Q.D2

**TABLE 4-11
EXTENT TO WHICH IMPROPER DISCLOSURE WAS HARMFUL (PUBLIC)**

Q.: Did you feel that you or the family member were embarrassed or harmed by that disclosure, or not?

Base: Medical information was disclosed in a manner considered improper

	Total	Race/Ethnicity			Income				
		White	Black	Hispanic	\$15,000 or Less	\$15,001 to \$35,000	\$35,001 to \$50,000	\$50,001 to \$75,000	\$75,001 and Over
Base	271	223	30	21	48	90	42	48	33
	%	%	%	%	%	%	%	%	%
Yes	31	30	35	21	40	29	34	30	15
No	65	67	52	75	49	69	64	69	85
Not sure	5	4	12	4	10	3	2	1	-

Have Asked A Physician To Record A Different Diagnosis

Despite the concerns by the public about the confidentiality of medical records, virtually no one says they have ever asked a doctor not to write down their health problem in their medical record or asked the doctor to put a less serious or less embarrassing diagnosis into the record than was actually the condition. (TABLE 4-12)

Q.H3

TABLE 4-12
ASKING PHYSICIAN TO RECORD A DIFFERENT DIAGNOSIS (PUBLIC)

Q.: Have you ever asked a doctor not to write down your health problem in your medical record, or asked the doctor to put a less serious or embarrassing diagnosis into the record than was actually the condition?

	Total
Base	1000
	%
Yes	1
No	99
Not sure	*

*Less than 0.5%.

How Serious Are Violations Of Confidentiality

Most of the leaders believe that violation of medical records' confidentiality is a serious problem in America today. Nearly 6 of 10 leaders say the problem is very or somewhat serious, but only 18% believe it is very serious. Again nurses express the most concern in seeing the problem as serious, with HMO CEOs being the least concerned. (TABLE 4-13)

Q.M5

TABLE 4-13
HOW SERIOUS ARE VIOLATIONS OF MEDICAL RECORDS' CONFIDENTIALITY (LEADERS)

Q.: How serious a problem do you think the violation of medical records' confidentiality is in America today — very serious, somewhat serious, not very serious, or not serious at all?

	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physicians	Nurses	Medical Society Heads	State Regulators	State Legislators	Congressional Aides	Human Resources Execs
Base	651	101	50	31	100	50	50	30	68	70	101
	%	%	%	%	%	%	%	%	%	%	%
Very serious	18	15	10	10	25	26	16	7	29	20	12
Somewhat serious	41	46	38	42	37	52	38	57	38	43	37
Not very serious	36	34	42	42	33	16	46	33	29	37	49
Not at all serious	4	6	10	6	5	4	-	3	1	-	3
Not sure	*	-	-	-	-	2	-	-	1	-	-

*Less than 0.5%.

Are Leaders Aware Of Violations And Did Violations Involve Manual Or Computerized Records

Each leadership group was asked about specific violations of which they were aware. About one-fourth (24%) of all leaders say they are aware of violations of the confidentiality of individuals' medical records from inside an organization that embarrassed or harmed the individual. Specifically, responding to the types of records involved, one-half of the leaders say the violations involved both manual and computerized records. Slightly over one third (35%) report the violations involved only manual records, and 8% of the leaders say the violations involved only computerized records. (TABLES 4-14 and 4-15)

Q.M6

TABLE 4-14
WHETHER AWARE OF VIOLATIONS OF
MEDICAL RECORDS' CONFIDENTIALITY (LEADERS)

Q.: Are you aware of any violations of the confidentiality of individuals' medical records from inside an organization that embarrassed or harmed the individual whose records were involved?

	Total Leaders
Base	651 %
Yes	24
No	76
Not sure	*

*Less than 0.5%.

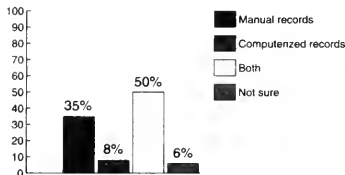
Q.M7

TABLE 4-15
WHETHER VIOLATION INVOLVED MANUAL OR COMPUTERIZED RECORDS (LEADERS)

Q.: Did these violations of medical records' confidentiality involve manual records, computerized records, or both?

Total Leaders %

Base: 155



What Kinds Of Records Were Improperly Disclosed

Test results or diagnostic reports are the types of records named by the largest percentage of leaders (37%). Only 6% of the leaders are aware of violations that involved psychiatric records and the same percentage give the answer for "HIV/AIDS information." (TABLE 4-16)

Q.M8

TABLE 4-16
TYPES OF MEDICAL RECORDS DISCLOSED (LEADERS)

Q.: What kinds of medical records were involved?

Base: Aware of violations in Q.M6.

	Total Leaders
Base:	155 %
Test results/diagnostic reports	37
Psychiatric records	6
Medical records	23
HIV/AIDS Information	6
Medical history	7
Insurance claims	4
Don't know	19

Who Revealed Information

According to the 24% of leaders who were aware of violations, hospital or laboratory employees or nurses were the most likely (22%) to have revealed the information. Individuals or institutions dealing with direct patient care are blamed more frequently than other institutions that maintain confidential medical data, such as employers, health insurers or government organizations. (TABLE 4-17)

Q.M9

TABLE 4-17
SOURCE OF INFORMATION VIOLATING MEDICAL
RECORDS' CONFIDENTIALITY (LEADERS)

Q.: Who revealed the information?

	Total Leaders
Base	155
	%
Hospital/lab employee/nurse	22
Non-hospital employee: doctor, insurance office	16
Hospital	15
Health insurer	10
Physician	10
Employer	3
Local government employee	2
Government employee	1
Federal government employee	1
State government employee	1
Other	15
Not sure	12

How Was Individual Embarrassed Or Harmed

These same leaders, aware of violations of the confidentiality of medical records that embarrassed or harmed the individual, were asked "how was the individual harmed?" Nearly one in four of the leaders say the individual was at the very least embarrassed by the violation. On some occasions the leaders also believe the individual suffered real harm. They report that the individual was denied health insurance (12%), lost a job (7%), was denied a job (6%) or was denied coverage (6%). (TABLE 4-18)

Q-M10

TABLE 4-18
HARM TO THE INDIVIDUAL WHOSE MEDICAL
RECORD'S CONFIDENTIALITY WAS VIOLATED (LEADERS)

Q.: How was the individual harmed?

Base: Aware of violations of medical records confidentiality

	Total Leaders
Base	155
	%
He/she was embarrassed	39
Denied health insurance	12
Lost job	7
Denied job	6
Denied coverage	6
Damaged reputation	5
Denied promotion	3
Denied reimbursement for claims	2
Denied medical procedures	-
Other	24
Not sure	6

CHAPTER 5: Information Technology

Concern About Medical Records On Computers

Many health care providers use computers for patient billing, accounting, laboratory work and storage of patient data. Computerization is still increasing, and computer programs are becoming more sophisticated and intricate. The public and leaders were asked about their concern with computer use in the health care field. One fifth of all adults are at least somewhat concerned about computer usage, and approximately one person in ten is very concerned. Forty percent are not concerned at all.

Most leaders do not share these concerns. Only 8% of leaders feel very concerned, while an additional 21% are somewhat concerned; 40% have absolutely no concern. Physicians (15%) and hospital CEOs (14%) express the greatest amount of concern of those leaders who say they are "very concerned." In contrast, HMO CEOs (52%), medical society heads (50%), and state regulators (50%) lead the group who say they are "not concerned at all." (TABLE 5-1)

Computer Problems In Health Care Profession

The public is concerned that problems are occurring because of the use of computers. The leaders tend to agree but to a lesser extent than the public:

- "Medical information is given to people who are not supposed to see it." (64% of the public thinks this happens very or somewhat often, compared to 43% of the leaders.)
- "Mistakes in a medical condition or problem are put into patients' records." (60% of the public believes this happens frequently versus 36% of the leaders.)
- "Mistakes are made in charges for health services." (75% of the public believes this happens at least somewhat often compared to 67% of the leaders.) (TABLE 5-2)

**TABLE 5-1
EXTENT CONCERNED ABOUT USE OF COMPUTERS BY HEALTH CARE PROVIDERS (PUBLIC)**

Q.: How concerned are you that many health care providers use today employ computers in some of their operations, such as patient billing and accounting, laboratory work, and keeping some medical records — are you very concerned, somewhat concerned, not too concerned, or not concerned at all?

	Total Public	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physicians	Nurses	Medical Society Heads	State Regulators	State Legislators	Congressional Aides	Human Resources Execs
Base	1000 %	651 %	101 %	50 %	31 %	100 %	50 %	50 %	30 %	68 %	70 %	101 %
Very concerned	8	18	14	-	3	15	12	2	3	7	6	3
Somewhat concerned	21	32	19	24	23	24	36	6	3	25	16	22
Not very concerned	31	25	27	24	39	35	20	42	43	25	30	35
Not concerned at all	40	25	41	52	35	25	32	50	50	43	49	41
Not sure	*	1	-	-	-	1	-	-	-	-	-	-

*Less than 0.5%.

Q.K2

TABLE 5-2
PROBLEMS CAUSED BY COMPUTERS

Q.: How often do you believe that any of the following problems are happening because computers are being used today by health care providers (READ EACH ITEM) do you think that occurs — very often, somewhat often, not very often or not often at all?

	PUBLIC					LEADERS				
	Very Often	Some-what Often	Not Very Often	Not Often At All	Not Sure	Very Often	Some-what Often	Not Very Often	Not Often At All	Not Sure
Base: 1000/651	%	%	%	%	%	%	%	%	%	%
Mistakes are made in charges for health services	32	43	20	4	1	22	45	26	6	1
Medical information is given to people who are not supposed to see it	22	42	26	7	4	9	34	45	10	1
Mistakes in a medical condition or problem are put into patients' records	16	44	32	6	2	5	31	50	13	1

Importance Of Review Organizations Having Privacy Policies

Many government agencies, employers and insurers hire information-processing organizations to review medical records in order to analyze treatments, results and costs. Both the leaders (93%) and the public (83%) think it is very important that these review organizations should have detailed privacy and confidentiality policies. Seventy-six percent of the leaders say having such policies is very important, compared to just over half of the public (54%). (TABLE 5-3)

Selection Of Organizations Handling Medical Records Based On Proven Record

When it comes to the selection of information-processing organizations, the public and leaders agree strongly on the importance of privacy protection experience. Nearly everyone (94% of the public and 97% of the leaders) thinks it is very or somewhat important that an organization is selected based on a proven record of protecting the confidentiality and security of personal records. This criterion could become an important factor in the administration of health care and management of health costs and quality in any national health care reform. (TABLE 5-4)

TABLE 5-3
IMPORTANCE OF REVIEW ORGANIZATIONS HAVING DETAILED PRIVACY AND CONFIDENTIALITY POLICIES

Q: Government agencies, employers and insurers hire information-processing organizations to review individual medical records in order to analyze treatments, results and costs. How important do you think it is for such review organizations to have detailed privacy and confidentiality policies — very important, somewhat important, not very important, or not at all important?

	Total Public	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physicians	Nurses	Medical Society Heads	State Regulators	State Legislators	Congressional Aides	Human Resources Execs
Base	1000 %	651 %	101 %	50 %	31 %	100 %	50 %	50 %	30 %	68 %	70 %	101 %
Very important	54	76	89	82	81	74	58	72	90	69	79	69
Somewhat important	29	17	9	14	16	14	26	22	7	22	17	24
Not very important	8	4	2	4	-	6	8	2	-	6	3	5
Not at all important	7	3	-	-	3	6	8	4	3	1	1	1
Not sure	2	*	-	-	-	-	-	-	-	1	-	1

*Less than 0.5%.

Q.K4

TABLE 5-4
IMPORTANCE OF RECORD OF CONFIDENTIALITY
IN SELECTING REVIEW ORGANIZATIONS

Q.: How important is it that such organizations should be selected on the basis of a proven record of protecting the confidentiality and security of the personal records they handle — very important, somewhat important, not very important, or not at all important?

	Total Leaders	Total Public
Base	651	1000
	%	%
Very important	80	74
Somewhat important	17	20
Not very important	2	3
Not at all important	1	2
Not sure	1	1

Whether Computerization Can Increase Records' Confidentiality

Leaders are divided in their opinions on whether increased computerization will result in the increased confidentiality of medical records. Fifty percent of leaders feel it "could be managed to strengthen confidentiality" with state regulators (63%), health insurer CEOs (61%), and congressional aides (60%) leading this group. Physicians (74%) and nurses (50%) stand out among the leaders (45%) who say this increased computerization is "almost certain to weaken confidentiality." (TABLE 5-5)

TABLE 5-5
CAN INCREASED COMPUTERIZATION OF MEDICAL AND HEALTH RECORDS
BE MANAGED TO INCREASE THE RECORD'S CONFIDENTIALITY (LEADERS)

Q.: In general, do you think the increased computerization of medical and health records could be managed to help strengthen the confidentiality of such records, or do you think computerization is almost certain to weaken confidentiality?

	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physi- cians	Nurses	Medical Society Heads	State Regu- lators	State Legis- lators	Congres- sional Aides	Human Resource Execs
Base	651 %	101 %	50 %	31 %	100 %	50 %	50 %	30 %	68 %	70 %	101 %
Could be managed to strengthen confidentiality	50	53	48	61	26	46	44	63	57	60	55
Almost certain to weaken confidentiality	45	43	44	35	74	50	46	27	38	30	40
Not sure	5	4	8	3	-	4	10	10	4	10	5

CHAPTER 6: Life Insurance

How Acceptable Is It For Life Insurance Companies To Ask Various Questions

Majorities of the public and of leaders believe it is acceptable for insurance companies to obtain a wide range of health and lifestyle information about those applying for life insurance.

Insurance companies require medical and non-medical information about a person applying for individual life insurance to evaluate the possibility of early death. For the most part, the public and the leadership groups agree on the appropriateness of specific types of information being made available to insurers. The item found at least somewhat acceptable by the highest percentage (81%) of adults is "urine tests to detect the use of illegal drugs." Almost all leaders (92%) found it very or somewhat acceptable for a company to obtain information about "whether the person uses tobacco products," and 88% found it very or somewhat acceptable to obtain information "whether the person drinks alcohol and how much."

The lowest acceptance by both the public and leaders was reported for whether the person was ever turned down for life insurance and why.

Overall, a substantial majority of Americans and leaders favors an insurance company having the privilege to obtain these types of information to decide about issuing policies and determining premium levels. (TABLES 6-1 through 6-9)

Q.11

TABLE 6-1
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO
OBTAIN CERTAIN DATA ABOUT INSURANCE APPLICANTS (PUBLIC)

Q.: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant (READ EACH ITEM) — very acceptable, somewhat acceptable, not very acceptable, or not at all acceptable?

	Very Acceptable	Somewhat Acceptable	Not Very Acceptable	Not At All Acceptable	Not Sure
Base: 1000	%	%	%	%	%
Urine tests to detect the use of illegal drugs	54 (53)	27	6	13	1
Blood test to determine the presence of AIDS or if the individual is HIV positive	54 (50)	26	8	11	1
Medical history of past diseases and illnesses	38 (49)	41	10	11	1
Whether the person drinks alcohol and how much	36 (49)	36	12	15	*
Family history of diseases and illnesses a person might inherit	32 (37)	39	11	17	1
Whether the person uses tobacco products	32 (59)	35	13	19	1
Whether the person engages in dangerous sports or hobbies	28 (34)	36	14	20	2
Whether the person was ever turned down for life insurance and why	28 (27)	34	15	21	2

*Less than 0.5%.

Figures in parentheses are for all leadership groups combined who said "very acceptable."

TABLE 6-2
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO OBTAIN DATA ABOUT
WHETHER AN INSURANCE APPLICANT HAS A MEDICAL HISTORY OF PAST DISEASES AND ILLNESSES

Q: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant . . . medical history of past diseases and illnesses — very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Total Public	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physicians	Nurses	Medical Society Heads	State Registrars	State Legislators	Congressional Aides	Human Resource Execs
Base	1000 %	651 %	101 %	50 %	31 %	100 %	50 %	50 %	30 %	68 %	70 %	101 %
Very acceptable	38	49	45	44	77	56	26	60	37	47	30	62
Somewhat acceptable	41	36	40	46	19	31	58	28	23	38	44	30
Nor very acceptable	10	8	9	4	3	6	10	10	17	4	20	5
Nor acceptable at all	11	6	7	6	-	7	6	2	20	10	6	3
Nor sure	1	*	-	-	-	-	-	-	3	-	-	-

*Less than 0.5%.

TABLE 6-3
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO OBTAIN DATA ABOUT WHETHER
AN INSURANCE APPLICANT HAS A FAMILY HISTORY OF DISEASES AND ILLNESSES A PERSON MIGHT INHERIT

Q.: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant . . . family history of diseases and illnesses a person might inherit — very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Total Leaders	Total Public	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physi- cians	Nurses	Medical Society Heads	State Regi- strars	State Legis- lators	Congres- sional Aides	Human Resource Execs
Base	651 %	1000 %	101 %	50 %	31 %	100 %	50 %	50 %	30 %	68 %	70 %	101 %
Very acceptable	37	32	32	40	68	44	22	38	37	38	14	49
Somewhat acceptable	39	44	44	46	23	35	38	44	20	44	47	36
Not very acceptable	13	11	11	4	6	14	24	10	13	3	30	10
Not acceptable at all	11	14	14	10	3	7	16	8	30	15	7	6
Not sure	*	1	-	-	-	-	-	-	-	-	1	-

*Less than 0.5%.

TABLE 6-4
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO OBTAIN
DATA ABOUT AN INSURANCE APPLICANT BY A BLOOD TEST FOR AIDS

Q.: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant . . . blood test to determine the presence of AIDS or if the individual is HIV positive — very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Total Public	Total Leaders		Hospital CEOs		HMO CEOs		Health Insurer CEOs		Physicians	Nurses		Medical Society Heads		State Regulators		State Legislators		Congressional Aides		Human Resource Execs	
		651	101	50	31	50	32	19	77		50	42	50	50	30	56	33	56	70	101	70	101
Very acceptable	54	50	42	50	77	50	32	19	77	66	30	56	33	56	26	60	26	60	26	60	26	60
Somewhat acceptable	26	29	40	32	19	32	40	19	23	23	36	28	23	28	39	23	24	39	39	23	39	23
Not very acceptable	8	8	8	2	-	2	8	-	4	4	18	12	13	12	23	5	3	23	23	5	23	5
Not acceptable at all	11	12	11	14	3	14	11	3	7	7	16	4	30	4	16	12	16	13	13	12	13	12
Not sure	1	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-

*Less than 0.5%.

TABLE 6-5
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO OBTAIN DATA ABOUT WHETHER AN INSURANCE APPLICANT WAS EVER TURNED DOWN FOR LIFE INSURANCE AND WHY

Q.: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant . . . whether the person was ever turned down for life insurance and why — very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Total Public	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physicians	Nurses	Medical Society Heads	State Regulators	State Legislators	Congressional Aides	Human Resource Execs
Base	1000	651	101	50	31	100	50	50	30	68	70	101
	%	%	%	%	%	%	%	%	%	%	%	%
Very acceptable	28	27	21	30	58	30	14	22	23	22	13	45
Somewhat acceptable	34	36	32	42	39	38	42	38	17	41	40	30
Not very acceptable	15	19	20	18	3	19	18	26	23	15	31	11
Not acceptable at all	21	18	28	10	-	13	26	14	33	21	16	15
Not sure	2	*	-	-	-	-	-	-	3	1	-	-

*Less than 0.5%.

**TABLE 6-6
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO OBTAIN DATA
ABOUT WHETHER AN INSURANCE APPLICANT USES TOBACCO PRODUCTS**

Q.: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant . . . whether the person uses tobacco products — very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Total Public	Total Leaders		Hospital CEOs		HMO CEOs		Health Insurer CEOs		Physicians		Nurses		Medical Society Heads		State Regulators		State Legislators		Congressional Aides		Human Resource Execs	
		651	101	50	31	100	50	30	68	50	50	50	30	68	70	101	68	74	47	53	47	70	101
	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Base	32	59	50	68	74	68	74	68	50	50	74	47	53	47	64								
Very acceptable	35	33	37	22	26	28	28	38	22	37	40	44	31										
Somewhat acceptable	13	4	6	6	-	2	2	2	4	7	-	6	3										
Not very acceptable	19	4	7	4	-	2	10	-	10	7	3	2											
Not acceptable at all																							
Not sure	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

TABLE 6-7
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO OBTAIN
DATA ABOUT WHETHER AN INSURANCE APPLICANT DRINKS ALCOHOL AND HOW MUCH

Q.: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant . . . whether the person drinks alcohol and how much — very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Total Public	Total Leaders		Health			Medical		State		Congressional		Human Resource	
		1000 %	651 %	HMO CEOs	Hospital CEOs	Insurer CEOs	Physicians	Nurses	Society Heads	Regulators	Legislators	Aides	Execs	%
Base	1000	651	101	50	31	100	50	50	30	68	70	101		
	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Very acceptable	36	49	41	52	55	63	50	50	43	47	33	52		
Somewhat acceptable	36	39	42	38	35	32	38	40	33	44	57	31		
Not very acceptable	12	7	8	6	6	3	8	6	10	4	3	12		
Not acceptable at all	15	5	10	4	3	2	4	4	10	4	7	5		
Not sure	*	*	-	-	-	-	-	-	3	-	-	-		

*Less than 0.5%.

TABLE 6-8
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO OBTAIN URINE TESTS TO DETECT AN INSURANCE APPLICANT'S USE OF ILLEGAL DRUGS

Q.: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant . . . urine tests to detect the use of illegal drugs — very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Total Public	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physicians	Nurses	Medical Society Heads	State Regulators	State Legislators	Congressional Aides	Human Resource Execs
Base	1000	651	101	50	31	100	50	50	30	68	70	101
	%	%	%	%	%	%	%	%	%	%	%	%
Very acceptable	54	53	52	46	68	66	44	54	37	53	36	62
Somewhat acceptable	27	31	35	36	23	26	32	34	33	34	37	26
Not very acceptable	6	7	5	8	10	2	12	8	7	6	17	6
Not acceptable at all	13	8	7	10	-	6	12	4	20	7	10	6
Not sure	1	•	1	-	-	-	-	-	3	-	-	-

• Less than 0.5%.

TABLE 6-9
EXTENT IT IS ACCEPTABLE FOR LIFE INSURANCE COMPANIES TO OBTAIN DATA ABOUT
WHETHER AN INSURANCE APPLICANT ENGAGES IN DANGEROUS SPORTS OR HOBBIES

Q.: When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether or not to issue the policy and at what price. How acceptable is it or the life insurance company to obtain the following types of information about the applicant . . . whether the person engages in dangerous sports or hobbies — very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Total Public	Total Leaders		Hospital CEOs		HMO CEOs		Health Insurer CEOs		Physicians		Nurses		Medical Society Heads		State Regulators		State Legislators		Congressional Aides		Human Resource Execs	
		%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%	%
Base	1000	651	101	50	31	100	50	31	100	50	30	68	70	101	50	30	68	70	101	50	30	68	70
Very acceptable	28	34	29	38	71	36	26	34	27	31	10	48	56	34	50	41	56	34	50	41	56	34	
Somewhat acceptable	36	43	48	34	19	48	44	50	50	50	41	56	34	50	41	56	34	50	41	56	34	50	
Not very acceptable	14	13	12	18	6	9	16	10	10	13	21	12	12	10	13	15	13	7	10	13	15	7	
Not acceptable at all	20	10	12	10	3	7	14	6	3	7	14	6	3	6	13	15	13	7	10	13	15	7	
Not sure	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

CHAPTER 7: Employment

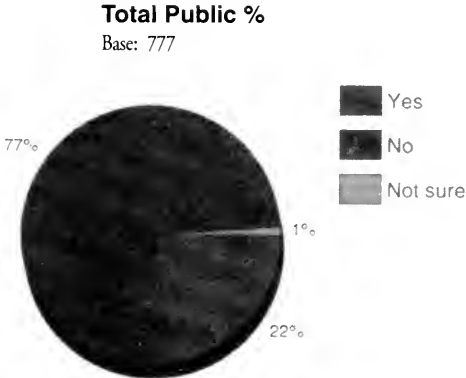
Are Americans Concerned About Changing Jobs And Losing Health Coverage

Of the 134 million adults (74%) who have been employed in the past five years, almost one-fourth (22%) are concerned about losing their health coverage if they change jobs. When these same people were asked if they have/had coverage at their current/last job, 32% say they did not. (TABLES 7-1 and 7-2)

Q:J2

TABLE 7-1
CONCERN OVER CHANGING JOBS AND LOSING HEALTH COVERAGE (PUBLIC)

Q.: Have you ever been concerned about changing jobs because you might not be able to get health insurance with a new employer, or not?



QJ3

TABLE 7-2
HEALTH COVERAGE THROUGH WORK (PUBLIC)

Q.: Does/Did a health insurance program or health plan cover you at your current/last job, or not?

Base: Currently employed or employed in past five years

	Total
Base	777
	%
Yes	67
No	32
Not sure	*

*Less than 0.5%.

Does Information Provided Affect Job Status

A substantial number of Americans are concerned about information provided in regard to medical claims under their health plan where they work.

Slightly more than 4 of 10 Americans are very or somewhat concerned that their job opportunities or job status might be affected if their medical claims information were to be seen by their employers.

An even higher percentage of leaders (57%) are concerned about job status or limited job opportunities if their claims information were seen by their employers. (TABLE 7-3)

TABLE 7-3
DEGREE OF CONCERN ABOUT CONFIDENTIALITY OF CLAIMS INFORMATION AT WORK

Q.: How concerned are you that medical claims information you provide under a health plan at work might be seen by your employer and used to limit your job opportunities or to affect your job status — are you very concerned, somewhat concerned, not very concerned, or not at all concerned?

Base (public only): Is currently employed or has been in the past five years and is/was covered by a health insurance program or health plan at their current/last job.

	Total Public	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physicians	Nurses	Medical Society Heads	State Registrars	State Legislators	Congressional Aides	Human Resource Execs
Base	500	651	101	50	31	100	50	50	38	68	70	101
	%	%	%	%	%	%	%	%	%	%	%	%
Very concerned	22	28	34	14	29	36	34	30	23	44	16	16
Somewhat concerned	19	29	28	26	26	35	26	28	37	28	29	27
Not very concerned	19	24	20	36	35	20	20	24	20	13	30	27
Not at all concerned	38	19	18	24	10	8	20	18	20	15	26	30
Not sure	1	*	1	-	-	1	-	-	-	-	-	1

*Less than 0.5%.

Concerns About Filing Medical Claims

Eight percent of those covered by a health plan in their current or last job were concerned about filing a claim because they were worried about medical information being known by a supervisor or someone else at work. This is quite a small percentage and reflects considerable trust in the employer's proper handling of such claims. (TABLE 7-4)

Q.J5

**TABLE 7-4
CONCERN OVER SUPERVISOR OR CO-WORKER LEARNING
OF TREATMENT IF CLAIM IS FILED (PUBLIC)**

Q.: Have you ever been concerned about filing a claim under your health plan at work because you did not want a supervisor or someone else at your workplace to know the treatment you received?

Base: Has/had health insurance coverage at current/last job.

	Total
Base:	536
	%
Yes	8
No	92
Not sure	-

Should Employers Have Information About Number Of Claims Filed

The public is divided on the issue of whether it is acceptable for an employer to know which employees are heavy users of the company's health plan. While 51% feel it is very or somewhat acceptable, 48% say it is not very or not at all acceptable.

In the aggregate, leaders' opinions parallel those of the public; however, there is a great deal of divergence among the various leadership groups. Congressional aides (41%), HMO CEOs (40%), and nurses (40%) lead the groups that find this practice "not at all acceptable" compared to state regulators (26%) and hospital CEOs (18%). (TABLE 7-5)

TABLE 7-5
**EXTENT IT IS ACCEPTABLE FOR AN EMPLOYER TO OBTAIN DATA SHOWING WHICH
 EMPLOYEES ARE HEAVY USERS OF A HEALTH PLAN**

Q: How acceptable is it for employers to obtain claims information showing which of their employees are heavy users of the company's health plan — very acceptable, somewhat acceptable, not very acceptable, or not at all acceptable?

	Total Public	Total Leaders		Hospital CEOs		HMO CEOs		Health Insurer CEOs		Physicians		Nurses		Medical Society Heads		State Regulators		Congressional Aides		Human Resource Excs			
		Count	%	Count	%	Count	%	Count	%	Count	%	Count	%	Count	%	Count	%	Count	%	Count	%		
Base	1000	651	65.1%	101	10.1%	50	5.0%	31	3.1%	100	10.0%	50	5.0%	50	5.0%	30	3.0%	68	6.8%	70	7.0%	101	10.1%
Very acceptable	19	18	94.7%	30	163.2%	12	63.2%	10	52.6%	17	89.5%	6	31.6%	10	52.6%	30	163.2%	18	94.7%	3	15.4%	27	134.3%
Somewhat acceptable	32	31	96.9%	33	103.1%	26	81.3%	32	100.0%	34	106.3%	28	87.7%	24	75.0%	23	71.9%	43	134.4%	31	96.9%	25	78.1%
Not very acceptable	17	21	123.5%	20	117.6%	20	117.6%	19	111.8%	22	129.4%	26	150.0%	30	176.5%	20	117.6%	13	76.5%	23	134.4%	22	129.4%
Not at all acceptable	31	30	96.8%	18	58.1%	40	129.0%	39	122.9%	27	84.4%	40	125.0%	34	106.3%	27	84.4%	26	79.0%	41	125.8%	27	84.4%
Not sure	2	*	0.3%	-	0.0%	2	6.3%	-	0.0%	-	0.0%	-	0.0%	2	6.3%	-	0.0%	-	0.0%	1	3.1%	-	0.0%

*Less than 0.5%.

CHAPTER 8: Health Care Reform

Importance of Selected Factors

With a national health care program being debated by the President and Congress, a set of topics was presented to respondents in order to measure those that they consider most important for a “good national health care program.” Six factors were considered:

- detecting health care providers who engage in fraud
- controlling health care costs
- protecting the confidentiality of people’s medical records
- providing health care insurance for those who do not have it today
- providing better data for research into diseases and treatments
- reducing current paperwork burdens on patients and providers

Generally, at a common-sense level, the expectation would be that all these factors are important contributors to a national health care program. The research confirms this, with more than three quarters of the public and leaders finding all six factors to be very important or essential.

“Protecting the confidentiality of peoples’ medical records” ranked third out of six for both the public and leaders in being “absolutely essential” to a good national health care program, ahead of “providing health care insurance for those who don’t have it today,” “reducing paperwork burdens,” or “providing better data for research.”

The public and leaders differ in the relative importance that they attach to specific factors, particularly in gauging which factors are “absolutely essential.” For instance, leaders are much more concerned than the public in reducing current paperwork burdens: 41% of leaders say it is absolutely essential compared to 26% of the public. Leaders are also a little more emphatic about protecting the confidentiality of people’s medical records and about controlling health care costs.

The above distinctions must be viewed, however, in the context of the overall importance ascribed to all six factors. In this sense “detecting health care fraud” and “controlling health care costs” are seen to be slightly more critical than other factors. (TABLE 8-1)

TABLE 8-1
RELATIVE IMPORTANCE OF CERTAIN TOPICS TO A NATIONAL HEALTH CARE PROGRAM

Q: The President and Congress are working on programs for national health care reform. For each of the following topics, please tell me how important you feel this is to a good national health care program. (READ EACH ITEM) Is that absolutely essential, very important, somewhat important, not very important, or not at all important?

Base:	Absolutely Essential		Very Important		Somewhat Important		Not Very Important		Not At All Important		Not Sure	
	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %
Public-1000 Leaders-651	47	45	41	48	9	4	2	1	•	1	•	2
Detecting health care providers who engage in fraud												
Controlling health care costs	49	42	39	48	10	7	1	1	1	1	•	1
Protecting the confidentiality of peoples' medical records	43	36	37	49	17	12	2	1	•	1	•	•
Providing health insurance for those who do not have it today	38	34	41	47	19	14	2	2	•	2	1	1
Providing better data for research into diseases and treatments	32	35	46	51	20	11	2	2	•	1	•	1
Reducing current paperwork burdens on patients and providers	41	26	41	41	16	26	1	4	•	1	•	2

•Less than 0.5%.

Health Care And Privacy

Within the context of a strong conviction that health care reform is "one of the top domestic issues facing the nation today," both the public and leaders are highly sensitive to the issues of privacy and particularly to the changes in the use of personal information which a national health care system could produce.

Confidence in health professionals as guardians of private information is high: nine in ten leaders believe that the health care professionals they use are careful to keep medical information confidential and "not reveal it improperly."

There is considerable concern, however, that medical information is disseminated to organizations beyond those providing health care services and that protection of privacy could deteriorate with a national health care system. Specifically, 61% of leaders agree with the statement that their "medical information is being seen by many organizations beyond those that I go to for health care," while close to three-quarters (73%) *disagree* that "a person's medical privacy in a national health care system will probably be protected better than it is currently."

There is clear acknowledgment (by eight in ten leaders) that for health care to be managed more efficiently, record keeping and the applications of "advanced computer technology" will increase. Further, there is reasonable confidence (67% of Americans agreeing) that today's laws do protect the confidentiality of medical records. (TABLE 8-2)

Worry About Computers and Health Care Reform

With the expectation that computers will be used even more extensively to manage and monitor health care operations, the public and leaders are less worried about computer usage in general than they are about computers enabling outsiders to snoop into their medical records.

Less than one quarter of the leaders and of the public worry a "great deal" about computers monitoring operations under health care reform, with the public (23%) slightly more concerned than the leaders (20%). Physicians (39%) seem the most worried and lead the various groups in expressing a "great deal" of concern about this issue. They are followed by state legislators (31%). However, 47% of state regulators say they are "not at all" concerned about this issue. A similar lack of concern is also expressed by congressional aides (51%). (TABLE 8-3)

In contrast to these findings, leaders and the public are clearly concerned that "outsiders may be able to tap into the computers to obtain medical information for improper purposes." Forty-four percent of leaders say they are "very concerned" about this, as are 51% of the public. In fact, only about one in five of the public, and 30% of leaders, are not concerned. (TABLE 8-4)

TABLE 8-2
GENERAL STATEMENTS ABOUT HEALTH CARE AND PRIVACY

Q.: Please tell me for each of the following statements whether you agree strongly, agree somewhat, disagree somewhat or disagree strongly. (READ EACH ITEM)

	Agree Strongly		Agree Somewhat		Disagree Somewhat		Disagree Strongly		Not Sure	
	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %
Base: Public-1000 Leaders-651										
Reforming health care is one of the top domestic issues facing the nation today	74	66	19	23	5	7	2	4	*	1
I believe the health professionals I use are careful to keep my medical information confidential and not reveal it improperly	56	56	38	31	4	6	1	4	1	2
If we are to manage health care reform efficiently, we will have to increase record keeping and apply advanced computer technology	39	33	42	43	13	15	5	6	1	3
It concerns me that my medical information is being seen today by many organizations beyond those that I go to for health care services	29	32	32	29	29	22	9	14	2	4
There are strong laws today that protect the confidentiality of people's medical records against improper disclosure and unauthorized access	26	26	49	41	17	19	5	9	3	5
A person's medical privacy in a national health care system will probably be protected better than it is currently	5	21	18	33	45	26	28	17	4	3

*Less than 0.5%.

TABLE 8-4
CONCERN ABOUT CERTAIN IMPROPER USES OF COMPUTERIZED HEALTH CARE INFORMATION

Q.: How concerned are you (READ EACH ITEM) — very concerned, somewhat concerned, not very concerned, or not at all concerned?

	Very Concerned		Somewhat Concerned		Not Very Concerned		Not At All Concerned		Not Sure	
	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %	Leaders %	Public %
Base: Public-1000 Leaders-651										
That outsiders may be able to tap into the computers to obtain medical information for improper purposes	34	51	36	30	24	14	6	5	*	-
That a computerized health care information system will come to be used for many non-health care purposes	30	38	38	37	24	17	8	7	1	1
That persons using computers inside the health care system may disclose your information improperly	22	39	38	35	32	19	8	7	*	*

*Less than 0.5%.

CHAPTER 9: The Issue of Personal Identity Cards and Numbers

Acceptance Of A Personal Identity Card

President Clinton's September 1993 speech to Congress on health care reform (delivered incidentally, well after the field work for this project was completed) focused heavily on the idea of a personal identity card for health care purposes. This research confirms a high level of acceptance of such a card.

Eighty-seven percent of the leader group and 84% of the public feel that a personal identity card would be either "very acceptable" or "somewhat acceptable," with a majority of the leaders (52%) and somewhat less than a majority of the public (45%) saying it would be "very acceptable." Only thirteen percent of the leaders and fifteen percent of the public say that an ID card would be either "not very acceptable" or "not acceptable at all." (TABLE 9-1)

ID Number For National Health Care Purposes

A personal identity card might entail assigning a number unique to an individual, not unlike a Social Security number. Interestingly the prototype card President Clinton held up during his September 1993 speech had a number prominently displayed on it.

This research implies that the general public has mixed feelings about numbers being assigned to them: 57% express concern while 42% are not concerned. Leaders are much less concerned about this issue with only about a third expressing concern. (TABLE 9-2)

Social Security Number Versus New ID Number

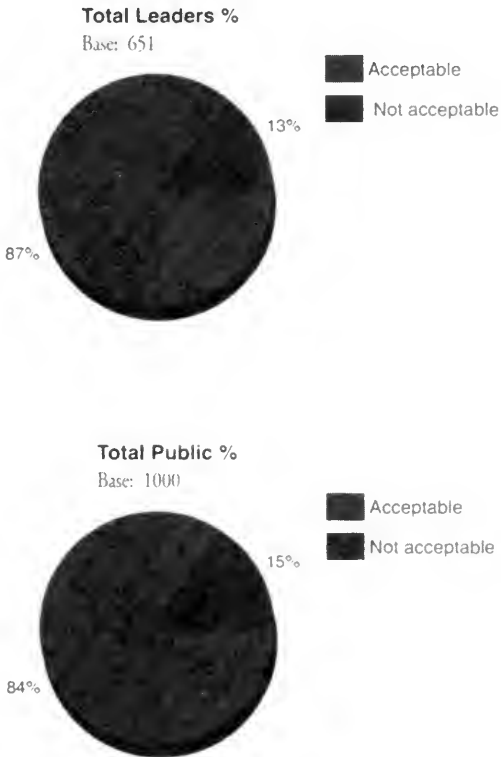
Were such a personal ID number introduced, there is clear preference for it being the same number as the Social Security number. A strong majority of leaders (72%) and the public (67%) favors using their Social Security number as their health care identification card. Less than a third of each group favor the issuing of a *new* number (i.e. distinct from Social Security) for this purpose. (TABLE 9-3)

Q.L3

TABLE 9-1

EXTENT A PERSONAL ID CARD IN A NATIONAL HEALTH PROGRAM IS ACCEPTABLE

Q.: A personal health insurance card has been proposed for accurate identification of persons in a national health care program and for general administration and so that everyone can show they are insured. How acceptable to you is such a personal identity card — very acceptable, somewhat acceptable, not very acceptable, not acceptable at all?



NOTE: A very large majority of all leadership groups feel that this would be acceptable to them.

TABLE 9-2
EXTENT OF CONCERN ABOUT AN ID NUMBER FOR NATIONAL HEALTH CARE PURPOSES

Q.: Under national health care reform, each person might be assigned an identification number for health insurance purposes. How concerned would you be to have such a health information number assigned to you — very concerned, somewhat concerned, not very concerned or not concerned at all?

	Total Public	Total Leaders		Hospital CEOs		HMO CEOs		Health Insurer CEOs		Physicians		Nurses		Medical Society Heads		State Regulators		State Legislative Aides		Congressional Aides		Human Resource Execs	
		1000 %	651 %	101 %	50 %	31 %	100 %	50 %	50 %	30 %	68 %	70 %	101 %	30 %	68 %	70 %	101 %	30 %	68 %	70 %	101 %		
Very concerned	28	11	17	4	6	14	10	12	10	19	6	7											
Somewhat concerned	29	23	22	14	13	30	28	14	17	25	33	19											
Not very concerned	22	29	26	30	39	26	36	32	33	24	29	31											
Not concerned at all	20	37	35	52	42	30	26	42	40	32	33	43											
Not sure/refused	1	*	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

*Less than 0.5%.

Q.15

TABLE 9-3
PREFERENCE OF SOCIAL SECURITY NUMBER OR NEW ID NUMBER AS NATIONAL HEALTH CARE ID NUMBER

Q.: If there were to be such a number, which would you prefer as an individual health number — your present Social Security number, or a new national health number assigned to each person?

	Total Public	Total Leaders		Hospital CEOs		HMO CEOs		Health Insurer CEOs		Physicians		Nurses		Medical Society Heads		State Regulators		State Legislative Aides		Congressional Aides		Human Resource Execs	
		1000 %	651 %	101 %	50 %	31 %	100 %	50 %	30 %	68 %	70 %	50 %	30 %	63 %	70 %	50 %	30 %	68 %	70 %	50 %	30 %	63 %	70 %
Your present Social Security Number	67	72	55	72	87	76	70	74	63	76	64	82											
A new national health number assigned to each person	30	26	43	28	13	22	30	22	30	19	33	17											
Not sure/refused	3	2	2	-	-	2	-	4	7	4	3	1											

CHAPTER 10: Privacy Legislation

Approaches To Safeguard The Confidentiality Of Medical Records

It is reasonable to expect that changes in the health care system will require adaptation of existing legislation affecting privacy and/or the introduction of new legislation. The degree to which respondents believe new legislation is needed will reflect the knowledge that leaders and the public have of and the confidence they place in current arrangements.

Respondents were therefore asked which approach they would prefer specifically to safeguard the confidentiality of medical records: enactment of new, comprehensive federal legislation to address this, or continuation of existing (state and federal) laws and professional business standards.

By a reasonable, but not overwhelming margin, leaders and the public favor enactment of new federal legislation that spells out rules for confidentiality of individual medical records. Approximately six of ten people from the leader (58%) and the public (56%) segments of the survey favor new legislation, compared to 41% of leaders and 39% of the general public who prefer "continuing with existing state and federal laws and professional standards." (TABLE 10-1)

Provisions For Federal Law On Confidentiality

Both the public and leaders agree by very large majorities that any new federal legislation should contain provisions specifically addressing confidentiality of medical information and records.

Two-thirds of the leaders (68%) and the public (69%) feel that it is "extremely important" that "all personal medical information in the health care system be designated as sensitive and penalties be imposed for unauthorized disclosures." Less than five percent of each group feel this statement is unimportant.

Three of four people in the leader groups (76%) and public (74%) feel that it is "extremely important" to clearly define who has access to medical records and what information could be obtained.

Slightly less than three quarters of the leaders (74%) and the public (72%) feel that it is "extremely important" that people have the right to inspect their medical records and that a procedure exists for them to correct or update them as required.

Public belief in the need for an independent national privacy board is strong, but not as marked as for the other provisions. On this issue, only slightly more than a quarter (28%) of the leaders feel it is "extremely important" that one be created, and only half of the public (46%) feels this way about it being created. The public (40%) and the leaders (41%) respond similarly, saying this issue is "somewhat important." (TABLES 10-2 through 10-6)

TABLE 10-1
PREFERRED APPROACH TO SAFEGUARD CONFIDENTIALITY

Q: If national health care reform is enacted, which one of these two approaches do you favor to safeguard the confidentiality of individual medical records in such a system?

	Total Public	Total Leaders	Hospital CEOs	HMO CEOs	Health Insurer CEOs	Physicians	Nurses	Medical Society Heads	State Regulators	State Legislators	Congressional Aides	Human Resource Execs
Base:	1000 %	651 %	101 %	50 %	31 %	100 %	50 %	50 %	30 %	68 %	70 %	101 %
Enact comprehensive federal legislation that spells out rules for confidentiality of individual medical records in such a system	56	58	65	54	45	50	60	58	60	54	66	61
OR												
Continue with existing state and federal laws and professional standards on confidentiality, disclosure and security	39	41	35	46	55	50	40	40	40	46	33	37
Not sure/refused	6	1	-	-	-	-	-	2	-	-	1	2

Q.L7

TABLE 10-2
IMPORTANCE OF CERTAIN PROVISIONS OF
A NEW FEDERAL CONFIDENTIALITY LAW (LEADERS)

Q.: Here are some provisions that are being discussed for a new federal law on confidentiality and uses of medical records. How important do you feel it is that (READ EACH ITEM) — extremely important, somewhat important, not very important or not important at all?

	Extremely Important %	Somewhat Important %	Not Very Important %	Not Important At All %	Not Sure %
Base: 651					
Rules would be spelled out as to who has access to medical records and what information could be obtained	76	20	2	2	*
Persons would have the right to inspect their medical records and have a procedure for correcting or updating them	74	22	2	2	*
All personal medical information in the health care system would be designated as sensitive, and penalties would be imposed for unauthorized disclosures	68	26	3	2	*
An independent National Medical Privacy Board would be created to hold hearings, issue regulations, and enforce standards	28	41	17	14	*

*Less than 0.5%.

QL7-1

TABLE 10-3
IMPORTANCE OF A PROVISION DESIGNATING MEDICAL INFORMATION
AS SENSITIVE IN A NEW FEDERAL CONFIDENTIALITY LAW

Q.: Here are some provisions that are being discussed for a new federal law on confidentiality and uses of medical records. How important do you feel it is that . . . all personal medical information in the health care system would be designated as sensitive, and penalties would be imposed for unauthorized disclosures — extremely important, somewhat important, not very important or not important at all?

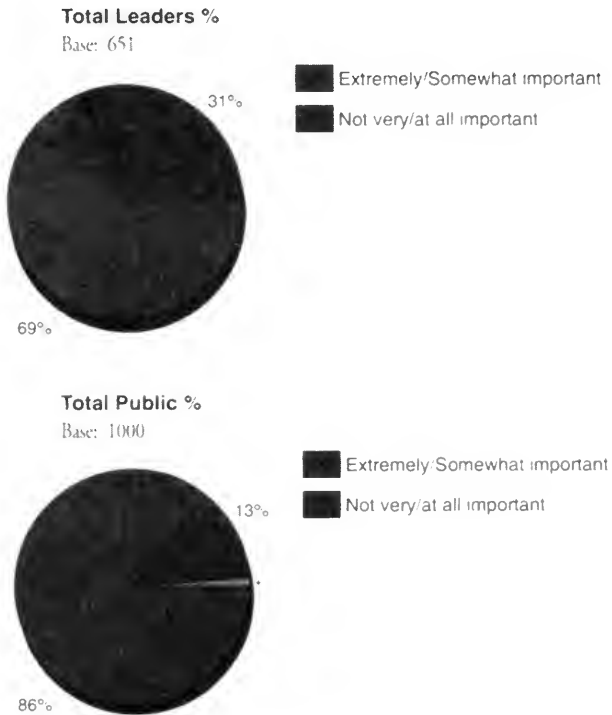
	Total Leaders	Total Public
Base	651 %	1000 %
Extremely important	68	69
Somewhat important	26	27
Not very important	3	2
Not at all important	2	1
Not sure	*	1

*Less than 0.5%.

Q.L7-2

TABLE 10-4
IMPORTANCE OF A PROVISION CREATING AN INDEPENDENT NATIONAL
MEDICAL PRIVACY BOARD IN A NEW FEDERAL CONFIDENTIALITY LAW

Q.: Here are some provisions that are being discussed for a new federal law on confidentiality and uses of medical records. How important do you feel it is that . . . an independent National Medical Privacy Board would be created, to hold hearings, issue regulations, and enforce standards — extremely important, somewhat important, not very important or not important at all?



*Less than 1%.

Q.L7-3

TABLE 10-5
IMPORTANCE OF A PROVISION IN A NEW FEDERAL CONFIDENTIALITY LAW
PROVIDING PERSONS THE RIGHT TO INSPECT THEIR MEDICAL RECORDS

Q.: Here are some provisions that are being discussed for a new federal law on confidentiality and uses of medical records. How important do you feel it is that . . . persons would have the right to inspect their medical records and have a procedure for correcting or updating them — extremely important, somewhat important, not very important or not important at all?

	Total Leaders	Total Public
Base	651 %	1000 %
Extremely important	74	72
Somewhat important	22	23
Not very important	2	2
Not at all important	2	2
Not sure	*	1

*Less than 0.5%.

Q.L7-4

TABLE 10-6
IMPORTANCE OF A PROVISION IN A NEW FEDERAL CONFIDENTIALITY LAW
RESTRICTING ACCESS TO MEDICAL RECORDS

Q.: Here are some provisions that are being discussed for a new federal law on confidentiality and uses of medical records. How important do you feel it is that . . . rules would be spelled out as to who has access to medical records and what information could be obtained — extremely important, somewhat important, not very important or not important at all?

	Total Leaders	Total Public
Base	651	1000
	%	%
Extremely important	76	74
Somewhat important	20	22
Not very important	2	3
Not at all important	2	1
Not sure	*	1

*Less than 0.5%.

CHAPTER 11: Leaders' Attitudes Toward Information and Procedures

Benefits From Access To Medical Information And Records

If intrusiveness is a perceived risk of increased computerization, what is its counterbalance? Are there perceived benefits to be derived from easier and more comprehensive access to medical information and records? The research invited opinions of leaders on this subject, specifically on outcomes research, practice pattern analysis, development of practice guidelines, and on the potential for reduction of fraud.

Generally, the leaders are confident that the quality of health care can be improved as a result of research derived from applying computerization to medical information. Physicians, however, are a little less confident than other leaders.

Nine of ten leaders feel that the quality of health care can be improved through outcomes research (research measuring the effectiveness of different therapies), either "a great deal" or "somewhat," with 43% saying "a great deal." State regulators (67%) and HMO CEOs (64%) said "a great deal" most frequently, and apparently are the most confident.

A third of the leaders (35%) feel that practice pattern analysis could improve the quality of health care "a great deal," with one half of all leaders (49%) saying it would improve quality "somewhat." Twenty-two percent of physicians, however, say that practice pattern analysis would improve quality "not very much."

Eighty-four percent of leaders think that the quality of health care can be improved through "the development of practice guidelines" "a great deal" or "somewhat," with 36% saying this would improve quality "a great deal." Almost four of ten physicians (36%) say that these guidelines would improve quality "not very much" or "not at all."

Eight of ten leaders (81%) say that "the reduction of fraud and abuse" would improve the quality of health care "a great deal" or "somewhat," with half of these eight leaders (39%) saying "a great deal." Interestingly, six of ten nurses say "a great deal" when responding to this question, compared to about a quarter of physicians. (TABLES 11-1, 11-2, 11-3, 11-4)

TABLE 11-1
EXTENT QUALITY OF HEALTH CARE CAN BE IMPROVED THROUGH OUTCOMES RESEARCH (LEADERS)

Q.: To what extent do you think the quality of health care can be improved through . . . outcomes research — a great deal, somewhat, not very much, or not all?

Base	Total Leaders	Hospital		HMO		Health Insurer		Physi- cians		Medical Society		State		Congress- ional		Human Resource	
		CEOs	%	CEOs	%	CEOs	%	Nurses	%	Heads	%	Legis- lators	%	Aides	%	Execs	%
	651	101	%	50	%	31	%	100	%	50	%	30	%	70	%	101	%
A great deal	43	47		64		55		26		44		67		40		38	
Somewhat	48	45		30		42		60		52		33		43		51	
Not very much	6	8		4		3		10		4		47		11		2	
Not at all	1	1		2		-		3		-		-		1		-	
Not sure	3	-		-		-		1		-		-		4		9	

TABLE 11-2
EXTENT QUALITY OF HEALTH CARE CAN BE IMPROVED THROUGH PRACTICE PATTERN ANALYSIS (LEADERS)

Q.: To what extent do you think the quality of health care can be improved through . . . practice pattern analysis — a great deal, somewhat, not very much, or not all?

Base	Total Leaders	Hospital CEOs		HMO CEOs		Health Insurer CEOs		Physicians		Nurses		Medical Society Heads		State Regulators		State Legislators		Congressional Aides		Human Resource Execs	
		101	%	50	%	31	%	100	%	50	%	30	%	68	%	70	%	101	%		
A great deal	35	50	54	26	11	28	28	60	32	33	38										
Somewhat	49	42	40	58	58	64	52	37	54	43	43										
Not very much	9	7	2	6	22	2	12	3	4	11	5										
Not at all	2	2	4	-	5	-	6	-	1	3	1										
Not sure	6	-	-	10	4	6	2	-	7	10	14										

Q.M1-3

TABLE 11-3
EXTENT QUALITY OF HEALTH CARE CAN BE IMPROVED THROUGH
THE DEVELOPMENT OF PRACTICE GUIDELINES (LEADERS)

Q.: To what extent do you think the quality of health care can be improved through . . . the development of practice guidelines — a great deal, somewhat, not very much, or not at all?

	Total Leaders	Hospital		HMO		Health Insurer CEOs		Physi- cians	Nurses	Medical Society Heads		State Regu- lators		State Legis- lators		Congres- sional Aides		Human Resource Execs	
		CEOs	%	CEOs	%	CEOs	%			CEOs	%	Heads	%	Regu- lators	%	Legis- lators	%	Aides	%
Base	651	101	%	50	%	31	%	100	50	50	%	30	%	68	%	70	%	101	%
A great deal	36	50		66		39		9	34	32		57		35		29		34	
Somewhat	48	38		30		55		55	58	60		40		46		47		50	
Not very much	10	9		2		3		23	2	4		3		15		16		8	
Not at all	5	4		2		-		13	6	4		-		4		4		3	
Not sure	2	-		-		3		-	-	-		-		-		4		6	

TABLE 11-4
**EXTENT QUALITY OF HEALTH CARE CAN BE IMPROVED
 THROUGH THE REDUCTION OF FRAUD AND ABUSE (LEADERS)**

Q.: To what extent do you think the quality of health care can be improved through . . . the reduction of fraud and abuse — a great deal, somewhat, not very much, or not at all?

	Total Leaders	Hospital CEOs		HMO CEOs		Health Insurer CEOs		Physi- cians		Nurses		Medical Society Heads		State Regu- lators		State Legis- lators		Congress- ional Aides		Human Resource Execs	
			%		%		%		%		%		%		%		%		%		%
Base	651	101	%	50	%	31	%	100	%	50	%	50	%	30	%	68	%	70	%	101	%
A great deal	39	29		26		52		28		60		20		40		50		36		53	
Somewhat	42	45		46		26		39		34		54		47		43		44		42	
Not very much	15	23		20		19		23		4		26		7		6		17		4	
Not at all	4	4		8		3		10		2		-		7		1		1		1	
Not sure	*	-		-		-		-		-		-		-		-		1		-	

Cost Reduced Through Procedures

With general confidence that improved procedures will lead to better health care, a question of cost arises. Leaders were asked whether improvements in the four procedures (fraud and abuse reduction, outcomes research, development of practice guidelines, and practice pattern analysis) could also help to reduce costs.

Thirty-seven percent of the leaders believe that the cost of health care can be reduced "a great deal" through "the reduction of fraud and abuse." The leaders also think, but not as strongly, that health care costs can also be reduced "a great deal" with "the development of practice guidelines (28%)," "outcomes research (28%)," and "practice analysis (26%)." (TABLE 11-5)

Q.M2

**TABLE 11-5
EXTENT COST OF HEALTH CARE CAN BE
REDUCED THROUGH CERTAIN ACTIVITIES (LEADERS)**

Q.: To what extent do you think the cost of health care can be reduced through (READ EACH ITEM) — a great deal, somewhat, not very much, or not at all?

	A Great Deal %	Somewhat %	Not Very Much %	Not At All %	Not Sure %
Base: 651					
The reduction of fraud and abuse	37	46	15	1	*
The development of practice guidelines	28	50	15	5	1
Outcomes research	28	55	13	2	3
Practice pattern analysis	26	52	13	4	6

*Less than 0.5%.

Satisfaction With Quality Of Data

Some experts have suggested, and these leaders apparently agree, that for cost reductions and health care improvements to take place, the quality and quantity of data available for those activities will need substantial improvement. Only five percent of the leaders are “very satisfied” with the quality of data on procedures, with approximately a third of leaders reporting being “not very satisfied.” Leaders respond similarly when asked about the quantity of data available, with slightly lower figures on “not very satisfied” responses. (TABLES 11-6 and 11-7)

Q.M3A

**TABLE 11-6
SATISFACTION WITH THE QUALITY OF THE DATA
AVAILABLE FOR CERTAIN ACTIVITIES (LEADERS)**

Q.: How satisfied are you with the quality of the data currently available for (READ EACH ITEM) — very satisfied, somewhat satisfied, not very satisfied, or not at all satisfied?

Base: 651	Very Satisfied %	Somewhat Satisfied %	Not Very Satisfied %	Not At All Satisfied %	Not Sure %
The reduction of fraud and abuse	5	39	36	13	7
The development of practice guidelines	5	45	33	10	7
Outcomes research	4	45	32	11	9
Practice pattern analysis	4	41	34	11	11

Q.M3B

**TABLE 11-7
SATISFACTION WITH THE QUANTITY OF THE DATA
AVAILABLE FOR CERTAIN ACTIVITIES (LEADERS)**

Q.: How satisfied are you with the quantity of the data currently available for (READ EACH ITEM) — very satisfied, somewhat satisfied, not very satisfied, or not at all satisfied?

Base: 651	Very Satisfied %	Somewhat Satisfied %	Not Very Satisfied %	Not At All Satisfied %	Not Sure %
The reduction of fraud and abuse	5	39	36	13	7
The development of practice guidelines	5	45	33	10	7
Outcomes research	4	45	32	11	9
Practice pattern analysis	4	41	34	11	11

TABLES

Table	Page
CHAPTER 1: PERSONAL PRIVACY IN AMERICA TODAY	
1-1 Public Concern About Threats To Personal Privacy.....	23
1-2 Leaders' Concern About Threats To Personal Privacy.....	25
1-3 Agreement Or Disagreement With Certain Statements About Business, Technology and Government	26
1-4 Distrust Index	27
1-5 Extent Public Is Concerned About Threats To Personal Privacy Correlated With 1993, 1990 And 1978 Distrust Index	29
1-6 Public Agreement Or Disagreement With Certain Statements Concerning Privacy.....	30
1-7 Extent To Which Public Agrees That Future Use Of Computers Must be Restricted To Preserve Privacy.....	32
1-8 Extent To Which Public Agrees Computers Have Improved The Quality Of Life	33
CHAPTER 2: ATTITUDES AND EXPERIENCES OF THE AMERICAN PUBLIC WITH HEALTH CARE AND MEDICAL RECORDS	
2-1 Health (Public)	34
2-2 Whether Public Has A Particular Place To Go When Sick Or Needs Advice About Health.....	35
2-3 How Much Is Known About The Contents Of An Individual's Medical Record	36
2-4 Whether Asked To See Their Medical Record (Public).....	38
2-5 Reason For Asking To See Their Record (Public)	39
2-6 Whether Their Medical Record Was Inspected (Public)	39
2-7 Reason Given For Refusing To Provide Medical Record (Public)	40

Table	Page
2-8 Whether Their Medical Record Was Understood (Public)	40
2-9 Importance Of Having The Legal Right To Obtain A Copy Of An Individual's Medical Record (Public)	41
CHAPTER 3: USES OF MEDICAL INFORMATION FOR MARKETING AND RESEARCH	
3-1 How Acceptable It Is To Use Certain Medical Information (Pharmacist) About Individuals Without Obtaining Their Prior Approval (Public)	43
3-2 How Acceptable It Is To Use Certain Medical Information (Fund Raising) About Individuals Without Obtaining Their Prior Approval (Public)	44
3-3 Whether Permission Should Be Required Before Medical Records Are Used For Research (Public)	45
3-4 Whether Permission Should Be Required Before Medical Records Are Used For Research Each Time (Public)	46
CHAPTER 4: DISCLOSURE OF CONFIDENTIAL INFORMATION AND MEDICAL RECORDS	
4-1 Perceived Level Of Concern About Threats To Medical Record's Confidentiality (Leaders)	47
4-2A Some Specific Medical Experiences (Public)	48
4-2B Whether Public Avoided Care Because Of Potential Harm To Job Or Other Opportunities	49
4-3 Reasons For Not Submitting Medical Claims (Public)	50
4-4 Whether Personal Medical Information Was Ever Improperly Disclosed (Public)	51
4-5 Whether Personal Medical Information Was Ever Improperly Disclosed (Public) (Doctor)	52
4-6 Whether Personal Medical Information Was Ever Improperly Disclosed (Public) (Clinic/Hospital)	53

Table	Page
4-7 Whether Personal Medical Information Was Ever Improperly Disclosed (Public) (Employer)	54
4-8 Whether Personal Medical Information Was Ever Improperly Disclosed (Public) (Pharmacy)	55
4-9 Whether Personal Medical Information Was Ever Improperly Disclosed (Public) (Health Insurer)	56
4-10 Whether Personal Medical Information Was Ever Improperly Disclosed (Public) (Public Health Agency)	57
4-11 Extent To Which Improper Disclosure Was Harmful (Public)	58
4-12 Asking Physician To Record A Different Diagnosis (Public)	59
4-13 How Serious Are Violations Of Medical Records' Confidentiality (Leaders)	60
4-14 Whether Aware Of Violations Of Medical Records' Confidentiality (Leaders)	61
4-15 Whether Violation Involved Manual Or Computerized Records (Leaders)	61
4-16 Types Of Medical Records Disclosed (Leaders)	62
4-17 Source Of Information Violating Medical Records' Confidentiality (Leaders)	63
4-18 Harm To The Individual Whose Medical Record's Confidentiality Was Violated (Leaders)	64
 CHAPTER 5: INFORMATION TECHNOLOGY	
5-1 Extent Concerned About Use Of Computers By Health Care Providers (Public)	66
5-2 Problems Caused By Computers (Public)	67
5-3 Importance Of Review Organizations Having Detailed Privacy And Confidentiality Policies	69

Table	Page
5-4 Importance Of Record Of Confidentiality In Selecting Review Organizations	70
5-5 Can Increased Computerization Of Medical And Health Records Be Managed To Increase The Record's Confidentiality (Leaders)	71
 CHAPTER 6: LIFE INSURANCE	
6-1 Extent It Is Acceptable For Life Insurance Companies To Obtain Certain Data About Insurance Applicants (Public)	73
6-2 Extent It Is Acceptable For Life Insurance Companies To Obtain Data Whether An Insurance Applicant Has A Medical History Of Past Diseases And Illness.....	74
6-3 Extent It Is Acceptable For Life Insurance Companies To Obtain Data Whether An Insurance Applicant Has A Family History Of Diseases And Illness A Person Might Inherit.....	75
6-4 Extent It Is Acceptable For Life Insurance Companies To Obtain Data About An Insurance Applicant By A Blood Test For AIDS.....	76
6-5 Extent It Is Acceptable For Life Insurance Companies To Obtain Data Whether An Insurance Applicant Was Ever Turned Down For Life Insurance And Why.....	77
6-6 Extent It Is Acceptable For Life Insurance Companies To Obtain Data Whether An Insurance Applicant Uses Tobacco Products.....	78
6-7 Extent It Is Acceptable For Life Insurance Companies To Obtain Data Whether An Insurance Applicant Drinks Alcohol And How Much.....	79
6-8 Extent It Is Acceptable For Life Insurance Companies To Obtain Urine Tests To Detect An Insurance Applicant's Use Of Illegal Drugs	80
6-9 Extent It Is Acceptable For Life Insurance Companies To Obtain Data Whether An Insurance Applicant Engages In Dangerous Sports Or Hobbies	81
 CHAPTER 7: EMPLOYMENT	
7-1 Concern Over Changing Jobs And Losing Health Coverage (Public).....	82
7-2 Health Coverage Through Work (Public).....	83

Table	Page
7-3 Degree Of Concern About Confidentiality Of Claims Information At Work	84
7-4 Concern Over Supervisor Or Co-worker Learning Of Treatment If Claim Is Filed (Public)	85
7-5 Extent It Is Acceptable For An Employer To Obtain Data Showing Which Employees Are Heavy Users Of A Health Plan (Public)	86
CHAPTER 8: HEALTH CARE REFORM	
8-1 Relative Importance Of Certain Topics To A National Health Care Program	88
8-2 General Statements About Health Care And Privacy	90
8-3 Extent Of Concern About The Use Of Computers In Health Care Operations	91
8-4 Concern About Certain Improper Uses Of Computerized Health Care Information	92
CHAPTER 9: THE ISSUE OF PERSONAL IDENTITY CARDS AND NUMBERS	
9-1 Extent A Personal ID Card In A National Health Program Is Acceptable	94
9-2 Extent Of Concern About An ID Number For National Health Care Purposes	95
9-3 Preference Of Social Security Number Or New ID Number As National Health Care ID Number	96
CHAPTER 10: PRIVACY LEGISLATION	
10-1 Preferred Approach To Safeguard Confidentiality	98
10-2 Importance Of Certain Provisions Of A New Federal Confidentiality Law (Leaders)	99
10-3 Importance Of A Provision Designating Medical Information As Sensitive In A New Federal Confidentiality Law	100
10-4 Importance Of A Provision Creating An Independent National Medical Privacy Board In A New Federal Confidentiality Law	101

Table	Page
10-5 Importance Of A Provision Providing Persons The Right To Inspect Their Medical Records In A New Federal Confidentiality Law.....	102
10-6 Importance Of A Provision Restricting Access To Medical Records In A New Federal Confidentiality Law.....	103
CHAPTER 11: LEADERS' ATTITUDES TOWARD INFORMATION AND PROCEDURES	
11-1 Extent Quality Of Health Care Can Be Improved Through Outcomes Research (Leaders).....	105
11-2 Extent Quality Of Health Care Can Be Improved Through Practice Pattern Analysis (Leaders).....	106
11-3 Extent Quality Of Health Care Can Be Improved Through The Development Of Practice Guidelines (Leaders).....	107
11-4 Extent Quality Of Health Care Can Be Improved Through The Reduction Of Fraud And Abuse (Leaders).....	108
11-5 Extent Cost Of Health Care Can Be Reduced Through Certain Activities (Leaders).....	109
11-6 Satisfaction With The Quality Of The Data Available For Certain Activities (Leaders).....	110
11-7 Satisfaction With The Quantity Of The Data Available For Certain Activities (Leaders).....	110
APPENDIX A: SURVEY METHODOLOGY	
A-1 Demographic Composition Of The Sample.....	119
APPENDIX B: QUESTIONNAIRES	

APPENDIX A: SURVEY METHODOLOGY

Sample Design: Public

Between July 26 and August 26, 1993, interviews were conducted with a cross section of 1,000 Americans eighteen years of age and older.

The Louis Harris and Associates Inc. National Telephone Sample is based on a methodology that is designed to produce representative samples of persons in telephone households in the 48 continental United States. The Harris National Telephone Sample makes use of random-digit selection procedures which assure sample representation of persons in households which are "listed" in telephone directories, as well as persons in households which are "unlisted" in telephone directories. The sample design is also explicitly designed to assure proper representation of households in central city, suburban, and rural areas within each of the 48 continental states.

The Harris National Telephone Sample is selected by a three-stage, stratified sampling process. The ultimate result of this process is a set of sample selections (phone numbers). In order to assure that the maximum degree of sample control is maintained, the basic sample design has been set up to produce cross-sectional national samples in increments of 500, 1,000, or 1,250 sampling points (i.e., households).

The representativeness of the sample is shown in Table A-1.

*Some households are "unlisted" as the result of a request for an unlisted number by the telephone subscriber. Other households are "unlisted" in the published directory because the telephone number was assigned after the publication date of the directory. Samples that are restricted to directory-listed numbers only may contain serious sample biases because of the exclusion of the various types of unlisted households.

TABLE A-1
DEMOGRAPHIC COMPOSITION OF THE PUBLIC SAMPLE

	1993		
	Number In Sample 1000	Unweighted Percentage 100	Weighted Percentage 100
Total			
Region			
East	238	24	22
Midwest	245	25	24
South	314	31	35
West	203	20	20
Size of Place			
Cities	331	33	34
Rest of Metropolitan Area	446	45	42
Outside of Metropolitan Area	223	22	24
Age			
18-29 years	238	24	24
30-49 years	433	43	41
50 and over	325	33	34
Education			
Less than high school	79	8	21
High school graduate	336	34	35
Some college	274	27	19
College graduate	202	20	19
Post graduate	107	11	6
Race			
White	857	86	85
Black	94	9	10
Hispanic	45	5	8
Sex			
Male	474	47	48
Female	526	53	52
Income (total household income)			
Under \$15,000	184	18	23
\$15,001-\$35,000	357	36	37
\$35,001-\$50,000	161	16	14
\$50,001-\$75,000	130	13	11
\$75,001 and over	96	10	8
Not sure/refused	-	-	7

NOTE: Subgroup totals do not always come to 1,000 because of some non-response.

East includes: Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont and West Virginia.

Midwest includes: Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin.

South includes: Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas and Virginia.

West includes: Arizona, California, Colorado, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming.

EXPLANATION OF WEIGHTED PERCENTAGES

- RACE:** Weighted percentages for this category add up to 103% because adults who consider themselves Hispanic may also consider themselves either White or Black. Those respondents who identify themselves as both Hispanic and either White or Black in the cross-tabulations are counted in both racial categories.
- INCOME:** Weighted percentages for this category add up to 93% because 7% chose not to provide data about their household income.

WEIGHTING

All national public cross sections are weighted to the Census Bureau's latest population parameters on region, education, sex, race, and age. This adjusts these key variables, where necessary, to their actual proportions in the population. Only moderate weighting is necessary in Harris samples.

SAMPLING ERROR

The results achieved from all sample surveys are subject to sampling error. Sampling error is defined as the difference between the results obtained from the sample and those that would have been obtained had the entire relevant population been surveyed. The size of the sampling error varies both with the size of the sample and with the percentage giving a particular answer. In a sample size of 1,000 interviews, in 95 cases out of 100, the sampling error is 3%.

SAMPLE DESIGN: LEADERSHIP

Between July 27 and August 5, 1993, interviews were conducted with 651 leaders:

- 101 Hospital CEOs or senior administrators whose facility has 100 or more beds and excludes federal and psychiatric facilities;
- 50 HMO CEOs or senior administrators;
- 31 commercial health insurer CEOs or senior executives;
- 100 physicians in the following specialties: general practice, family practice, internal medicine, pediatrics, and obstetrics/gynecology;
- 50 licensed registered nurses;
- 50 heads of state and national medical societies;
- 30 state health-care regulators;
- 68 state legislators who serve on health care committees;
- 70 aides to federal legislators on health care committees;
- 101 human resources executives who are their firm's most senior human resources or personnel executive.

APPENDIX B: QUESTIONNAIRES

I. Social and Privacy Policy Questions

- X1. How concerned are you about threats to your personal privacy in America today -- very concerned, somewhat concerned, not very concerned, not at all concerned?

Very concerned.....(15(49 -1
 Somewhat concerned..... 30 -2
 Not very concerned..... 11 -3
 Not at all concerned... 6 -4
 Not sure..... 3 -5

- X2. For each of the following statements, please tell me whether you tend to agree or disagree? (READ EACH ITEM)

<u>ROTATE -- START AT "X"</u>		<u>Agree</u>	<u>Disagree</u>	<u>Not</u>
				<u>Sure</u>
()	1. Technology has almost gotten out of control	(17(<u>50</u> -1	<u>47</u> -2	<u>3</u> -3
()	2. Government can generally be trusted to look after our interests	(18(<u>23</u> -1	<u>75</u> -2	<u>2</u> -3
()	3. The way one votes has no effect on what the government does	(19(<u>42</u> -1	<u>57</u> -2	<u>2</u> -3
()	4. In general, business helps us more than it harms us	(20(<u>69</u> -1	<u>27</u> -2	<u>4</u> -3

- X3. (READ EACH ITEM) Do you agree strongly, agree somewhat, disagree somewhat or disagree strongly?

<u>ROTATE -- START AT "X"</u>		<u>Agree</u>	<u>Agree</u>	<u>Disagree</u>	<u>Disagree</u>	<u>Not</u>
		<u>Strongly</u>	<u>Somewhat</u>	<u>Somewhat</u>	<u>Strongly</u>	<u>Sure</u>
()	1. My rights to privacy are adequately protected today by laws and organizational practices	(21(<u>9</u> -1	<u>31</u> -2	<u>29</u> -3	<u>29</u> -4	<u>2</u> -5
()	2. Consumers have lost all control over how personal information about them is circulated and used by companies	(22(<u>47</u> -1	<u>33</u> -2	<u>15</u> -3	<u>4</u> -4	<u>2</u> -5
()	3. Computers have improved the quality of life in our society	(23(<u>36</u> -1	<u>40</u> -2	<u>13</u> -3	<u>10</u> -4	<u>1</u> -5
()	4. If privacy is to be preserved, the use of computers must be sharply restricted in the future	(24(<u>40</u> -1	<u>31</u> -2	<u>17</u> -3	<u>10</u> -4	<u>2</u> -5

A. Personal Health Care Experiences

A1. Overall would you say your health is excellent, pretty good, fair, or poor?

Excellent.....	(25)	<u>36</u>	-1
Pretty good.....		<u>48</u>	-2
Fair.....		<u>13</u>	-3
Poor.....		<u>3</u>	-4
Not sure.....		<u>2</u>	-5

A2. (Have/do) you or (has/does) a member of your immediate family (READ ITEM), or not?

		Yes, No, Not			
		Has	Has Not	Sure	
<u>ROTATE -- START AT "X"</u>					
()	1. Ever had a serious illness such as a heart attack, stroke, or cancer	(26)	<u>35</u> -1	<u>65</u> -2	<u>1</u> -3
()	2. Have a long-term medical condition such as diabetes or epilepsy	(27)	<u>12</u> -1	<u>80</u> -2	<u>1</u> -3
()	3. Have any major physical or mental disabilities	(28)	<u>14</u> -1	<u>85</u> -2	<u>1</u> -3
()	4. Ever used the services of a psychologist, psychiatrist, or other mental-health professional	(29)	<u>22</u> -1	<u>77</u> -2	<u>1</u> -3
()	5. Ever wanted to seek services for a physical condition or mental health problem but didn't do so, because you didn't want to harm your job prospects or other life opportunities	(30)	<u>7</u> -1	<u>92</u> -2	<u>1</u> -3

B. Attitudes Toward and Experiences With Medical Records

- B1. Is there a particular clinic, health center, doctor's office or some other place where you go when you are sick or need advice about your health?

Yes.....(31(76 -1 (ASK Q.B2)
 No..... 24 -2 (SKIP TO Q.B8)
 Not sure..... * -3

- B2. How much do you know about the information that is in your medical record in that place? Would you say you know everything that is in it,
- or
- that you have a general idea but don't know in detail,
- or
- that you don't know anything about your records?

Know everything.....(32(25 -1
 Have a general idea but don't know in detail.. 62 -2
 Don't know anything..... 13 -3
 Not sure..... * -4

- B3. Have you ever asked your health care provider to show you your complete medical record, or not?

Yes.....(33(24 -1 (ASK Q.B4)
 No..... 76 -2 (SKIP TO Q.B8)
 Not sure..... * -3

- B4. What was your reason for asking to see your record? (PROBE FOR SPECIFICS)

Curiosity 44%; Need to transfer records, changed Doctors, moved 18%;
Need to see results of tests/treatment 13%; I'm a medical professional/Doctor/RN 2%;
Wanted copy for personal records 2%

- B5. Was your complete record shown to you or a copy of it given to you, or not?

Yes.....(34(92 -1 (ASK Q.B6)
 No..... 8 -2 (SKIP TO Q.B7)
 Not sure..... * -3

- B6. Did you understand it, or have it explained to you in a satisfactory way, or not?

Yes.....(35(97 -1
 No..... 3 -2
 Not sure..... * -3

(SKIP TO Q.B8)

- B7. What was the reason given for refusing to provide it to you? (PROBE FOR SPECIFICS)

Couldn't locate 31%; Gave no reason, just refused 25%

ASK EVERYONE

88. How important do you think it is that you should have the legal right to obtain a copy of your medical records -- very important, somewhat important, not very important, or not important at all?

Very important.....	(36	<u>84</u>	-1
Somewhat important.....		<u>12</u>	-2
Not very important.....		<u>1</u>	-3
Not at all important.....		<u>2</u>	-4
Not sure.....		<u>1</u>	-5

C. Opening Questions About Health Care Reform

- C1. The President and Congress are working on programs for national health care reform. For each of the following topics, please tell me how important you feel this is to a good national health-care program. (READ EACH ITEM) Is that absolutely essential, very important, somewhat important, not very important, or not at all important?

<u>ROTATE -- START AT "X"</u>	<u>Absolutely Essential</u>	<u>Very Important</u>	<u>Somewhat Important</u>	<u>Not Very Important</u>	<u>Not At All Important</u>	<u>Not Sure</u>
() 1. Providing health insurance for those who do not have it today (37(<u>34</u> -1	<u>47</u> -2	<u>14</u> -3	<u>2</u> -4	<u>2</u> -5	<u>1</u> -6	
() 2. Controlling health care costs (38(<u>42</u> -1	<u>48</u> -2	<u>7</u> -3	<u>1</u> -4	<u>1</u> -5	<u>1</u> -6	
() 3. Protecting the confidentiality of people's medical records (39(<u>36</u> -1	<u>49</u> -2	<u>12</u> -3	<u>1</u> -4	<u>1</u> -5	<u>*</u> -6	
() 4. Detecting health care providers who engage in fraud (40(<u>45</u> -1	<u>48</u> -2	<u>4</u> -3	<u>1</u> -4	<u>1</u> -5	<u>2</u> -6	
() 5. Providing better data for research into diseases and treatments (41(<u>35</u> -1	<u>51</u> -2	<u>11</u> -3	<u>2</u> -4	<u>1</u> -5	<u>1</u> -6	
() 6. Reducing current paperwork burdens on patients and providers (42(<u>26</u> -1	<u>41</u> -2	<u>26</u> -3	<u>4</u> -4	<u>1</u> -5	<u>2</u> -6	

C2. Please tell me for each of the following statements whether you agree strongly, agree somewhat, disagree somewhat, or disagree strongly? (READ EACH ITEM)

<u>ROTATE -- START AT "X"</u>		<u>Agree</u> <u>Strongly</u>	<u>Agree</u> <u>Somewhat</u>	<u>Disagree</u> <u>Somewhat</u>	<u>Disagree</u> <u>Strongly</u>	<u>Not</u> <u>Sure</u>
()	1. There are strong laws today that protect the confidentiality of people's medical records against improper disclosure and unauthorized access	(43) <u>26</u> -1	<u>41</u> -2	<u>19</u> -3	<u>9</u> -4	<u>5</u> -5
()	2. It concerns me that my medical information is being seen today by many organizations beyond those that I go to for health care services .	(44) <u>32</u> -1	<u>29</u> -2	<u>22</u> -3	<u>14</u> -4	<u>4</u> -5
()	3. Reforming health care is one of the top domestic issues facing the nation today	(45) <u>66</u> -1	<u>23</u> -2	<u>7</u> -3	<u>4</u> -4	<u>1</u> -5
()	4. I believe the health professionals I use are careful to keep my medical information confidential and not reveal it improperly	(46) <u>56</u> -1	<u>31</u> -2	<u>6</u> -3	<u>4</u> -4	<u>2</u> -5
()	5. If we are to manage health care reform efficiently, we will have to increase record-keeping and apply advanced computer technology	(47) <u>33</u> -1	<u>43</u> -2	<u>15</u> -3	<u>6</u> -4	<u>3</u> -5
()	6. A person's medical privacy in a national health care system will probably be protected better than it is currently	(48) <u>21</u> -1	<u>33</u> -2	<u>26</u> -3	<u>17</u> -4	<u>3</u> -5

D. Handling Medical Records and Health Information

D1. Do you believe that (READ EACH ITEM) has ever disclosed your personal medical information in a way that you felt was improper, or not?

<u>ROTATE -- START AT "X"</u>	<u>Yes</u>	<u>No</u>	<u>Not Sure</u>
() 1. A doctor who has treated you or a family member . . .	(49(<u>7</u> -1	<u>92</u> -2	<u>1</u> -3
() 2. A clinic or hospital that treated you or a family member	(50(<u>11</u> -1	<u>87</u> -2	<u>2</u> -3
() 3. Your employer or a family member's employer	(51(<u>9</u> -1	<u>89</u> -2	<u>1</u> -3
() 4. A pharmacy or druggist who filled a prescription for you or a family member	(52(<u>3</u> -1	<u>95</u> -2	<u>1</u> -3
() 5. Health Insurance companies	(53(<u>15</u> -1	<u>82</u> -2	<u>3</u> -3
() 6. Public health agencies	(54(<u>10</u> -1	<u>86</u> -2	<u>4</u> -3

ASK Q.D2 IF "YES" TO ANY ITEM IN Q.D1. OTHERS SKIP TO Q.E1.

D2. Did you feel that you or the family member were embarrassed or harmed by that disclosure, or not?

Yes.....	(56(<u>31</u> -1
No.....	<u>65</u> -2
Not sure.....	<u>3</u> -3

E. Medical Research

Medical researchers sometimes need to use individual patient records to study the causes of diseases or the value of specific drugs or treatments. However, they do not release any information identifying specific patients.

- E1. If you are not personally identified in any publication, should your permission be required before your medical records are used for research, or isn't that necessary?

Should be required.....(57(64-1 (GO TO Q.E2)

Isn't necessary.....35-2 } (SKIP TO Q.G1)

Not sure.....*-3

- E2. Should your permission be required each time a researcher seeks to use your medical records or would asking for general advance permission to use your records for medical research be sufficient?

Required each time.....(58(56-1

General permission is sufficient.....42-2

Not sure.....2-3

NOTE: Section F (Demographics) appears at the end of this questionnaire.

G. Use of Medical Information in Direct MarketingASK EVERYONE

G1. In the following situations, how acceptable do you think it is to use medical information about individuals without first obtaining approval from the individual? (READ EACH ITEM) Would this be very acceptable, somewhat acceptable, not very acceptable, not at all acceptable?

<u>ROTATE -- START AT "X"</u>	Very <u>Acceptable</u>	Somewhat <u>Acceptable</u>	Not Very <u>Acceptable</u>	Not At All <u>Acceptable</u>	Not <u>Sure</u>
() 1. Pharmacists providing the names and addresses of customers using certain medications to companies that want to mail out information about or offers of new medications for those conditions (59(<u>11</u> -1	<u>28</u> -2	<u>19</u> -3	<u>41</u> -4	<u>1</u> -5	
() 2. Hospital fund-raisers getting the names of those who have been patients at the hospital to write them for donations to the hospital (60(<u>6</u> -1	<u>27</u> -2	<u>27</u> -3	<u>47</u> -4	<u>*</u> -5	

H. Health Insurance

H1. I will read you a list of different kinds of health plans, insurance, or programs. Please tell me whether or not you are currently covered by this? (READ EACH ITEM)

ROTATE -- START AT "X"	Yes	No	Not Sure
() 1. Health insurance that you or a family member purchased directly	(61(<u>32</u> -1	<u>67</u> -2	<u>1</u> -3
() 2. Health insurance or a health program provided through your work, military service, union, or your spouse's work, military service or union	(62(<u>64</u> -1	<u>35</u> -2	<u>*</u> -3
() 3. Health care under a veterans program	(63(<u>5</u> -1	<u>94</u> -2	<u>1</u> -3
() 4. Medicare, the government program for persons over 65 and some disabled persons	(64(<u>19</u> -1	<u>81</u> -2	<u>*</u> -3
() 5. Medicaid, the government program for persons with low incomes	(65(<u>6</u> -1	<u>94</u> -2	<u>*</u> -3

READ LAST

6. Any other health insurance (SPECIFY):

_____ . . (66(2-1 97-2 *-3
 Any other health insurance (SPECIFY):
 _____ (67-69)

H2a. Have you or has a member of your immediate family ever personally paid for a medical test, treatment, or counseling rather than submit a bill or claim under a health plan or program?

Yes.....(70(25-1 (ASK Q.H2b)
 No..... 70-2 (SKIP TO Q.H3)
 Never had health insurance (vol.)... 3-3
 Not sure..... 2-4

H2b. Why was that?

Procedure not covered 24%; Easier, eliminates paperwork 24%; Did not have insurance 13%;
Wanted confidentiality/privacy 11%; Haven't met deductible 8%; Minor bill/procedure 8%
Needed quick medical attention 3%

H3. Have you ever asked a doctor not to write down your health problem in your medical record, or asked the doctor to put a less serious or embarrassing diagnosis into the record than was actually the condition?

Yes.....(71(1-1
 No..... 99-2
 Not sure..... *-3

I. Life Insurance

11. When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether or not to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant (READ EACH ITEM) -- very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all? ROTATE -- START AT "X"

	Very <u>Acceptable</u>	Somewhat <u>Acceptable</u>	Not Very <u>Acceptable</u>	Not <u>Acceptable</u> <u>At All</u>	Not <u>Sure</u>
(1).Medical history of past diseases and illnesses (72(<u>38</u> -1	<u>41</u> -2	<u>10</u> -3	<u>11</u> -4	<u>1</u> -5	
(2).Family history of diseases and illnesses a person might inherit (73(<u>32</u> -1	<u>39</u> -2	<u>11</u> -3	<u>17</u> -4	<u>1</u> -5	
(3).Blood test to determine the presence of AIDS or if the individual is HIV positive (74(<u>54</u> -1	<u>26</u> -2	<u>8</u> -3	<u>11</u> -4	<u>1</u> -5	
(4).Whether the person was ever turned down for life insurance and why (75(<u>28</u> -1	<u>34</u> -2	<u>15</u> -3	<u>21</u> -4	<u>2</u> -5	
(5).Whether or not the person uses tobacco products (76(<u>32</u> -1	<u>35</u> -2	<u>13</u> -3	<u>19</u> -4	<u>1</u> -5	
(6).Whether the person drinks alcohol and how much (77(<u>36</u> -1	<u>36</u> -2	<u>12</u> -3	<u>15</u> -4	<u>*</u> -5	
(7).Urine tests to detect the use of illegal drugs (78(<u>54</u> -1	<u>27</u> -2	<u>6</u> -3	<u>13</u> -4	<u>1</u> -5	
(8).Whether the person engages in dangerous sports or hobbies . . (79(<u>28</u> -1	<u>36</u> -2	<u>14</u> -3	<u>20</u> -4	<u>2</u> -5	

J. Employment

J1. Are you currently employed or have you been employed in the past 5 years, or not?

Yes.....(80(74-1 (ASK Q.J2)

No.....26-2 (SKIP TO Q.J6)

Not sure.....--3

J2. Have you ever been concerned about changing jobs because you might not be able to get health insurance with a new employer, or not?

Yes.....2*(08(22-1

No.....77-2

Not sure.....1-3

J3. Does/did a health insurance program or health plan cover you at your current/last job, or not?

Yes.....(09(67-1 (ASK Q.J4)

No.....32-2 (SKIP TO Q.J6)

Not sure.....*-3

J4. How concerned are you that medical claims information you provide under a health plan at work might be seen by your employer and used to limit your job opportunities or to affect your job status -- are you very concerned, somewhat concerned, not very concerned, or not at all concerned?

Very concerned....(10(22-1

Somewhat concerned....19-2

Not very concerned....19-3

Not at all concerned...38-4

Not sure.....1-5

J5. Have you ever been concerned about filing a claim under your health plan at work because you did not want a supervisor or someone else at your workplace to know the treatment you received?

Yes.....(11(8-1

No.....92-2

Not sure.....--3

ASK EVERYONE

J6. How acceptable is it for employers to obtain claims information showing which of their employees are heavy users of the company's health plan -- is that very acceptable, somewhat acceptable, not very acceptable, or not at all acceptable?

Very acceptable....(12(19-1

Somewhat acceptable...32-2

Not very acceptable...17-3

Not at all acceptable..31-4

Not sure.....2-5

K. Information Technology

- K1. How concerned are you that many health care providers you use today employ computers in some of their operations, such as patient billing and accounting, laboratory work, and keeping some medical records -- are you very concerned, somewhat concerned, not too concerned, not concerned at all?

Very concerned.....(13) 18 -1
 Somewhat concerned..... 32 -2
 Not too concerned..... 25 -3
 Not concerned at all..... 25 -4
 Not sure..... 1 -5

- K2. How often do you believe that any of the following problems are happening because computers are being used today by health care providers (READ EACH ITEM) -- do you think that occurs very often, somewhat often, not very often, not often at all?

ROTATE -- START AT "X"	Very Often	Somewhat Often	Not Very Often	Not Often At All	Not Sure
() 1. Mistakes are made in charges for health services	(14) <u>32</u> -1	<u>43</u> -2	<u>20</u> -3	<u>4</u> -4	<u>1</u> -5
() 2. Medical information is given to people who are not supposed to see it	(15) <u>22</u> -1	<u>42</u> -2	<u>26</u> -3	<u>7</u> -4	<u>4</u> -5
() 3. Mistakes in a medical condition or problem are put into patients' records	(16) <u>16</u> -1	<u>44</u> -2	<u>32</u> -3	<u>6</u> -4	<u>2</u> -5

- K3. Government agencies, employers and insurers hire information-processing organizations to review individual medical records in order to analyze treatments, results and costs. How important do you think it is for such review organizations to have detailed privacy and confidentiality policies -- very important, somewhat important, not very important or not at all important?

Very important.....(17) 54 -1
 Somewhat important..... 29 -2
 Not very important..... 8 -3
 Not at all important..... 7 -4
 Not sure..... 2 -5

- K4. How important is it that such organizations should be selected on the basis of a proven record of protecting the confidentiality and security of the personal records they handle -- very important, somewhat important, not very important, or not important at all?

Very important.....(18) 74 -1
 Somewhat important..... 20 -2
 Not very important..... 3 -3
 Not at all important..... 2 -4
 Not sure..... 1 -5

L. Policy Issues in National Health Care Reform

- L1. Under national health care reform, computers are expected to be used extensively to manage and monitor operations. Some of these uses will involve individual medical records. In general, would such use of computers worry you -- a great deal, a little or not at all?

A great deal.....(19) 23-1
 A little.....47-2
 Not at all.....29-3
 Not sure.....1-4

- L2. How concerned are you (READ EACH ITEM) very concerned, somewhat concerned, not very concerned or not concerned at all?

ROTATE -- START AT "X"	Very Concerned	Somewhat Concerned	Not Very Concerned	Not	
				At All Concerned	Not Sure
() 1. That persons using computers inside the health-care system may disclose your information improperly . . . (20)	<u>39</u> -1	<u>35</u> -2	<u>19</u> -3	<u>7</u> -4	<u>*</u> -5
() 2. That outsiders may be able to tap into the computers to obtain medical information for improper purposes (21)	<u>51</u> -1	<u>30</u> -2	<u>14</u> -3	<u>5</u> -4	<u>--</u> -5
() 3. That a computerized health-care information system will come to be used for many non-health care purposes (22)	<u>38</u> -1	<u>37</u> -2	<u>17</u> -3	<u>7</u> -4	<u>1</u> -5

- L3. A personal health insurance card has been proposed for accurate identification of persons in a national health care program and for general administration and so that everyone can show they are insured. How acceptable to you is such a personal identity card -- very acceptable, somewhat acceptable, not very acceptable, not acceptable at all?

Very acceptable....(23) 45-1
 Somewhat acceptable....39-2
 Not very acceptable....8-3
 Not acceptable at all...7-4
 Not sure.....1-5

- L4. Under national health-care reform, each person might be assigned an identification number for health insurance purposes. How concerned would you be to have such a health information number assigned to you -- very concerned, somewhat concerned, not very concerned or not concerned at all?

Very concerned....(24) 28-1
 Somewhat concerned....29-2
 Not very concerned....22-3
 Not concerned at all...20-4
 Not sure.....1-5

- L5. If there were to be such a number, which would you prefer as an individual health number -- your present Social Security Number, or a new national health number assigned to each person?

Your present Social Security Number.....(25(67 -1
 A new national health number assigned to each person... 30 -2
 Not sure..... 3 -3

26Z

- L6. If a national health care reform is enacted, which one of these two approaches do you favor to safeguard the confidentiality of individual medical records in such a system? (READ BOTH ITEMS)

ROTATE -- START AT "X"

- () 1. Enact comprehensive federal legislation that spells out rules for confidentiality of individual medical records in such a system . . . (27(56 -1

OR

- () 2. Continue with existing state and federal laws and professional standards on confidentiality, disclosure, and security 39 -2
 Not sure 6 -3

- L7. Here are some provisions that are being discussed for a new federal law on confidentiality and uses of medical records. How important do you feel it is that (READ EACH ITEM) -- extremely important, somewhat important, not very important, or not important at all?

<u>ROTATE -- START AT "X"</u>	Extremely Important	Somewhat Important	Not Very Important	Not	
				Important At All	Not Sure
() 1. All personal medical information in the health care system would be designated as sensitive, and penalties would be imposed for unauthorized disclosures (28(<u>69</u> -1	<u>27</u> -2	<u>2</u> -3	<u>1</u> -4	<u>1</u> -5	
() 2. Rules would be spelled out as to who has access to medical records and what information could be obtained . . (29(<u>74</u> -1	<u>22</u> -2	<u>3</u> -3	<u>1</u> -4	<u>1</u> -5	
() 3. Persons would have the right to inspect their medical records, and have a procedure for correcting or updating them (30(<u>72</u> -1	<u>23</u> -2	<u>2</u> -3	<u>2</u> -4	<u>1</u> -5	
() 4. An independent National Medical Privacy Board would be created, to hold hearings, issue regulations, and enforce standards (31(<u>46</u> -1	<u>40</u> -2	<u>7</u> -3	<u>6</u> -4	<u>1</u> -5	

32-55Z

F. Demographics

Now I have a few questions for classification purposes.

F1. How old are you? IF HESITANT, READ LIST

18 to 20.....	(56)	(<u>6</u> -1
21 to 24.....		<u>7</u> -2
25 to 29.....		<u>10</u> -3
30 to 34.....		<u>11</u> -4
35 to 39.....		<u>12</u> -5
40 to 44.....		<u>10</u> -6
45 to 49.....		<u>8</u> -7
50 to 64.....		<u>19</u> -8
65 to 74.....		<u>10</u> -9
75 and over.....	(57)	(<u>5</u> -0
Not sure.....		* -1

F2. What is the highest level of school you have completed or the highest degree you have received?

Less than high school (grades 1-11, grade 12 but no diploma.....	(58)	(<u>21</u> -1
High school graduate or equivalent (e.g. GED)....		<u>35</u> -2
Some college but no degree (incl. 2 year occupational or vocational programs).....		<u>19</u> -3
College graduate (e.g. BA, AB, BS).....		<u>19</u> -4
Post graduate (e.g. MA, MS, MEng, MEd, MSW, MBA, MD, DDe, DVM, LLB, JD, PhD, EdD).....		<u>6</u> -5
Not sure.....		* -6

F3. Regardless of how you might vote, what do you usually consider yourself -- a Republican, a Democrat, an independent, or what?

Republican.....	(59)	(<u>32</u> -1
Democrat.....		<u>40</u> -2
Independent.....		<u>21</u> -3
Other (vol.).....		<u>4</u> -4
Not sure.....		<u>4</u> -5

F4. How would you describe your own personal political philosophy -- conservative, moderate, or liberal?

Conservative.....	(60)	(<u>41</u> -1
Moderate.....		<u>40</u> -2
Liberal.....		<u>16</u> -3
Not sure.....		<u>3</u> -4

F5. Just over half the population voted in last November's presidential election. Many people didn't or couldn't vote. Were you able to vote last November or not?

Voted.....	(61)	(<u>75</u> -1 (ASK Q.F6)
Did not vote.....		<u>25</u> -2
Not sure.....		<u>-</u> -3 (SKIP TO Q.F7)
Refused.....		* -4

F6. Who did you vote for -- George Bush, Bill Clinton, Ross Perot or someone else?

George Bush.....	(62)	(<u>28</u> -1
Bill Clinton.....		<u>44</u> -2
Ross Perot.....		<u>17</u> -3
Someone else.....		<u>3</u> -4
Not sure/refused.....		<u>9</u> -5

n = 781

F7. Which of the following income categories best describes your total 1992 household income? Was it (READ LIST)?

\$7,500 or less.....	63	(<u>9</u>	-1	
\$7,501 to \$15,000.....			<u>14</u>	-2	INTERVIEWER: TOTAL HOUSEHOLD
\$15,001 to \$25,000.....			<u>23</u>	-3	INCOME BEFORE TAXES FROM ALL
\$25,001 to \$35,000.....			<u>15</u>	-4	SOURCES -- IF UNSURE OF 1992
\$35,001 to \$50,000.....			<u>14</u>	-5	INCOME, PROBE FOR ESTIMATE
\$50,001 to \$75,000.....			<u>11</u>	-6	
\$75,001 to \$100,000.....			<u>4</u>	-7	
\$100,001 or over.....			<u>4</u>	-8	
Not sure.....			<u>7</u>	-9	

F8. Are you of Hispanic origin or descent, or not?

Yes, of Hispanic origin.....	64	(<u>8</u>	-1
No, not of Hispanic origin.....			<u>91</u>	-2
Not sure.....			<u>1</u>	-3

F9. Do you consider yourself white, black or African American, Asian, or something else?

White.....	65	(<u>85</u>	-1
Black or African American.....			<u>10</u>	-2
Asian or Pacific Islander.....			<u>1</u>	-3
American Indian or Alaskan native.....			<u>*</u>	-4
Not sure.....			<u>3</u>	-5

That completes the interview. Thank you very much for your cooperation!

FROM OBSERVATION: Respondent Sex

Male.....	66	(<u>48</u>	-1
Female.....			<u>52</u>	-2

67-80Z

Time Ended: _____ A.M/P.M.

I. Social and Privacy Policy Questions

- X1. How concerned are you about threats to your personal privacy in America today -- very concerned, somewhat concerned, not very concerned, not at all concerned?

Very concerned.....(16) 33 -1
 Somewhat concerned..... 45 -2
 Not very concerned..... 17 -3
 Not at all concerned... 5 -4
 Not sure..... * -5

- X2. For each of the following statements, please tell me whether you tend to agree or disagree? (READ EACH ITEM)

<u>ROTATE -- START AT "X"</u>	<u>Agree</u>	<u>Disagree</u>	<u>Not Sure</u>
() 1. Technology has almost gotten out of control	(17) <u>26</u> -1	<u>73</u> -2	<u>1</u> -3
() 2. Government can generally be trusted to look after our interests	(18) <u>29</u> -1	<u>70</u> -2	<u>2</u> -3
() 3. The way one votes has no effect on what the government does	(19) <u>28</u> -1	<u>71</u> -2	<u>1</u> -3
() 4. In general, business helps us more than it harms us	(20) <u>87</u> -1	<u>11</u> -2	<u>2</u> -3

(There is no X3 in this version.)

(There is no A1-A2 in this version.)

21-36Z

(There is no B1-B8 in this version.)

C. Opening Questions About Health Care Reform

- C1. The President and Congress are working on programs for national health care reform. For each of the following topics, please tell me how important you feel this is to a good national health-care program. (READ EACH ITEM) Is that absolutely essential, very important, somewhat important, not very important, or not at all important?

ROTATE -- START AT "X"	Absolutely Essential	Very Important	Somewhat Important	Not Very Important	Not At All Important	Not Sure
() 1. Providing health insurance for those who do not have it today	(37) <u>38</u> -1	<u>41</u> -2	<u>19</u> -3	<u>2</u> -4	<u>*</u> -5	<u>1</u> -6
() 2. Controlling health care costs	(38) <u>49</u> -1	<u>39</u> -2	<u>10</u> -3	<u>1</u> -4	<u>1</u> -5	<u>*</u> -6
() 3. Protecting the confidentiality of people's medical records	(39) <u>43</u> -1	<u>37</u> -2	<u>17</u> -3	<u>2</u> -4	<u>*</u> -5	<u>*</u> -6
() 4. Detecting health care providers who engage in fraud	(40) <u>47</u> -1	<u>41</u> -2	<u>9</u> -3	<u>2</u> -4	<u>*</u> -5	<u>*</u> -6
() 5. Providing better data for research into diseases and treatments	(41) <u>32</u> -1	<u>46</u> -2	<u>20</u> -3	<u>2</u> -4	<u>*</u> -5	<u>*</u> -6
() 6. Reducing current paperwork burdens on patients and providers	(42) <u>41</u> -1	<u>41</u> -2	<u>16</u> -3	<u>1</u> -4	<u>*</u> -5	<u>*</u> -6

C2. Please tell me for each of the following statements whether you agree strongly, agree somewhat, disagree somewhat, or disagree strongly? (READ EACH ITEM)

<u>ROTATE -- START AT "X"</u>	<u>Agree Strongly</u>	<u>Agree Somewhat</u>	<u>Disagree Somewhat</u>	<u>Disagree Strongly</u>	<u>Not Sure</u>
() 1. There are strong laws today that protect the confidentiality of people's medical records against improper disclosure and unauthorized access	(43) <u>26</u> -1	<u>49</u> -2	<u>17</u> -3	<u>5</u> -4	<u>3</u> -5
() 2. It concerns me that my medical information is being seen today by many organizations beyond those that I go to for health care services	(44) <u>29</u> -1	<u>32</u> -2	<u>29</u> -3	<u>9</u> -4	<u>2</u> -5
() 3. Reforming health care is one of the top domestic issues facing the nation today	(45) <u>74</u> -1	<u>19</u> -2	<u>5</u> -3	<u>2</u> -4	<u>*</u> -5
() 4. I believe the health professionals I use are careful to keep my medical information confidential and not reveal it improperly	(46) <u>56</u> -1	<u>38</u> -2	<u>4</u> -3	<u>1</u> -4	<u>1</u> -5
() 5. If we are to manage health care reform efficiently, we will have to increase record-keeping and apply advanced computer technology (47) <u>39</u> -1	<u>42</u> -2	<u>13</u> -3	<u>5</u> -4	<u>1</u> -5	
() 6. A person's medical privacy in a national health care system will probably be protected better than it is currently	(48) <u>5</u> -1	<u>18</u> -2	<u>45</u> -3	<u>28</u> -4	<u>4</u> -5

(There is no D1-D2 in this version.)

(There is no E1-E2 in this version.)

49-71Z

(There is no G1-G2 in this version.)

(There is no H1-H3 in this version.)

I. Life Insurance

11. When persons apply for individual life insurance, the insurance company asks for medical and non-medical information to evaluate the possibility of early death. This information is used to determine whether or not to issue the policy and at what price. How acceptable is it for the life insurance company to obtain the following types of information about the applicant (READ EACH ITEM) -- very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all? ROTATE -- START AT "X"

	Very Acceptable	Somewhat Acceptable	Not Very Acceptable	Not Acceptable At All	Not Sure
() 1. Medical history of past diseases and illnesses (72(<u>49</u> -1	<u>36</u> -2	<u>8</u> -3	<u>6</u> -4	<u>*</u> -5	
() 2. Family history of diseases and illnesses a person might inherit (73(<u>37</u> -1	<u>39</u> -2	<u>13</u> -3	<u>11</u> -4	<u>*</u> -5	
() 3. Blood test to determine the presence of AIDS or if the individual is HIV positive (74(<u>50</u> -1	<u>29</u> -2	<u>8</u> -3	<u>12</u> -4	<u>*</u> -5	
() 4. Whether the person was ever turned down for life insurance and why (75(<u>27</u> -1	<u>36</u> -2	<u>19</u> -3	<u>18</u> -4	<u>*</u> -5	
() 5. Whether or not the person uses tobacco products (76(<u>59</u> -1	<u>33</u> -2	<u>4</u> -3	<u>4</u> -4	<u>-</u> -5	
() 6. Whether the person drinks alcohol and how much (77(<u>49</u> -1	<u>39</u> -2	<u>7</u> -3	<u>5</u> -4	<u>*</u> -5	
() 7. Urine tests to detect the use of illegal drugs (78(<u>53</u> -1	<u>31</u> -2	<u>7</u> -3	<u>8</u> -4	<u>*</u> -5	
() 8. Whether the person engages in dangerous sports or hobbies . . (79(<u>34</u> -1	<u>43</u> -2	<u>13</u> -3	<u>10</u> -4	<u>-</u> -5	

802

J. Employment

(There is no J1-J3 in this version.)

2* 8-9Z

- J4. How concerned are you that medical claims information you provide under a health plan at work might be seen by your employer and used to limit your job opportunities or to affect your job status -- are you very concerned, somewhat concerned, not very concerned, or not at all concerned?

Very concerned...	2*	10	28	-1
Somewhat concerned....		29	-2	
Not very concerned....		24	-3	
Not at all concerned...		19	-4	
Not sure.....		*	-5	

(There is no J5 in this version.)

2* 11Z

- J6. How acceptable is it for employers to obtain claims information showing which of their employees are heavy users of the company's health plan -- is that very acceptable, somewhat acceptable, not very acceptable, or not at all acceptable?

Very acceptable....	12	18	-1
Somewhat acceptable....	31	-2	
Not very acceptable....	21	-3	
Not at all acceptable...	30	-4	
Not sure.....	*	-5	

K. Information Technology

- K1. How concerned are you that many health care providers you use today employ computers in some of their operations, such as patient billing and accounting, laboratory work, and keeping some medical records -- are you very concerned, somewhat concerned, not too concerned, not concerned at all?

Very concerned.....(13(8 -1
 Somewhat concerned..... 21 -2
 Not too concerned..... 31 -3
 Not concerned at all..... 40 -4
 Not sure..... * -5

- K2. How often do you believe that any of the following problems are happening because computers are being used today by health care providers (READ EACH ITEM) -- do you think that occurs very often, somewhat often, not very often, not often at all?

ROTATE -- START AT "X"	Very Often	Somewhat Often	Not Very Often	Not Often At All	Not Sure
() 1. Mistakes are made in charges for health services	(14(<u>22</u> -1	<u>45</u> -2	<u>26</u> -3	<u>6</u> -4	<u>1</u> -5
() 2. Medical information is given to people who are not supposed to see it	(15(<u>9</u> -1	<u>34</u> -2	<u>45</u> -3	<u>10</u> -4	<u>1</u> -5
() 3. Mistakes in a medical condition or problem are put into patients' records	(16(<u>5</u> -1	<u>31</u> -2	<u>50</u> -3	<u>13</u> -4	<u>1</u> -5

- K3. Government agencies, employers and insurers hire information-processing organizations to review individual medical records in order to analyze treatments, results and costs. How important do you think it is for such review organizations to have detailed privacy and confidentiality policies -- very important, somewhat important, not very important or not at all important?

Very important.....(17(76 -1
 Somewhat important..... 17 -2
 Not very important..... 4 -3
 Not at all important..... 3 -4
 Not sure..... * -5

- K4. How important is it that such organizations should be selected on the basis of a proven record of protecting the confidentiality and security of the personal records they handle -- very important, somewhat important, not very important, or not important at all?

Very important.....(18(80 -1
 Somewhat important..... 17 -2
 Not very important..... 2 -3
 Not at all important..... 1 -4
 Not sure..... 1 -5

L. Policy Issues in National Health Care Reform

- L1. Under national health care reform, computers are expected to be used extensively to manage and monitor operations. Some of these uses will involve individual medical records. In general, would such use of computers worry you -- a great deal, a little or not at all?

A great deal.....(19) 20 -1
 A little..... 44 -2
 Not at all..... 35 -3
 Not sure..... 1 -4

- L2. How concerned are you (READ EACH ITEM) very concerned, somewhat concerned, not very concerned or not concerned at all?

		Very Concerned	Somewhat Concerned	Not Very Concerned	Not At All Concerned	Not Sure
ROTATE -- START AT "X"						
()	1. That persons using computers inside the health-care system may disclose your information improperly . . .	(20) <u>22</u> -1	<u>38</u> -2	<u>32</u> -3	<u>8</u> -4	<u>*</u> -5
()	2. That outsiders may be able to tap into the computers to obtain medical information for improper purposes	(21) <u>34</u> -1	<u>36</u> -2	<u>24</u> -3	<u>6</u> -4	<u>*</u> -5
()	3. That a computerized health-care information system will come to be used for many non-health care purposes	(22) <u>30</u> -1	<u>38</u> -2	<u>24</u> -3	<u>8</u> -4	<u>1</u> -5

- L3. A personal health insurance card has been proposed for accurate identification of persons in a national health care program and for general administration and so that everyone can show they are insured. How acceptable to you is such a personal identity card -- very acceptable, somewhat acceptable, not very acceptable, not acceptable at all?

Very acceptable....(23) 52 -1
 Somewhat acceptable.... 35 -2
 Not very acceptable.... 8 -3
 Not acceptable at all... 5 -4
 Not sure..... 1 -5

- L4. Under national health-care reform, each person might be assigned an identification number for health insurance purposes. How concerned would you be to have such a health information number assigned to you -- very concerned, somewhat concerned, not very concerned or not concerned at all?

Very concerned.....(24) 11 -1
 Somewhat concerned..... 23 -2
 Not very concerned..... 29 -3
 Not concerned at all... 37 -4
 Not sure..... * -5

- L5. If there were to be such a number, which would you prefer as an individual health number -- your present Social Security Number, or a new national health number assigned to each person?

Your present Social Security Number.....(25(72 -1
 A new national health number assigned to each person... 26 -2
 Not sure..... 2 -3

26Z

- L6. If a national health care reform is enacted, which one of these two approaches do you favor to safeguard the confidentiality of individual medical records in such a system? (READ BOTH ITEMS)

ROTATE -- START AT "X"

- () 1. Enact comprehensive federal legislation that spells out rules for confidentiality of individual medical records in such a system (27(58 -1

OR

- () 2. Continue with existing state and federal laws and professional standards on confidentiality, disclosure, and security 41 -2
 Not sure 1 -3

- L7. Here are some provisions that are being discussed for a new federal law on confidentiality and uses of medical records. How important do you feel it is that (READ EACH ITEM) -- extremely important, somewhat important, not very important, or not important at all?

ROTATE -- START AT "X"

	Extremely	Somewhat	Not Very	Not	Important	Not
	Important	Important	Important	At All	Sure	

- | | | | | | | |
|---|-------------------|--------------|--------------|--------------|-------------|--|
| () 1. All personal medical information in the health care system would be designated as sensitive, and penalties would be imposed for unauthorized disclosures | (28(<u>68</u> -1 | <u>26</u> -2 | <u>3</u> -3 | <u>2</u> -4 | <u>*</u> -5 | |
| () 2. Rules would be spelled out as to who has access to medical records and what information could be obtained | (29(<u>76</u> -1 | <u>20</u> -2 | <u>2</u> -3 | <u>2</u> -4 | <u>*</u> -5 | |
| () 3. Persons would have the right to inspect their medical records, and have a procedure for correcting or updating them | (30(<u>74</u> -1 | <u>22</u> -2 | <u>2</u> -3 | <u>2</u> -4 | <u>*</u> -5 | |
| () 4. An independent National Medical Privacy Board would be created, to hold hearings, issue regulations, and enforce standards | (31(<u>28</u> -1 | <u>41</u> -2 | <u>17</u> -3 | <u>14</u> -4 | <u>*</u> -5 | |

M. (Leaders Only) Value Attached to the Use of Statistical Data and Investigative Procedures

The next questions deal with statistical and investigative procedures used to analyze health care data.

- M1. To what extent do you think the quality of health care can be improved through (READ EACH ITEM) -- a great deal, somewhat, not very much, or not at all?

		Q.M1				
		A	Not			
		Great	Some-	Very	Not	Not
		Deal	what	Much	At All	Sure
()	1. Outcomes research	(32(<u>43</u> -1	<u>48</u> -2	<u>6</u> -3	<u>1</u> -4	<u>3</u> -5
()	2. Practice Pattern Analysis	(33(<u>35</u> -1	<u>49</u> -2	<u>9</u> -3	<u>2</u> -4	<u>6</u> -5
()	3. The development of practice guidelines	(34(<u>36</u> -1	<u>48</u> -2	<u>10</u> -3	<u>5</u> -4	<u>2</u> -5
()	4. The reduction of fraud and abuse	(35(<u>39</u> -1	<u>42</u> -2	<u>15</u> -3	<u>4</u> -4	<u>*</u> -5

- M2. To what extent do you think the cost of health care can be reduced through (READ EACH ITEM) -- a great deal, somewhat, not very much, or not at all?

		Q.M2				
		A	Not			
		Great	Some-	Very	Not	Not
		Deal	what	Much	At All	Sure
()	1. Outcomes research	(36(<u>28</u> -1	<u>55</u> -2	<u>13</u> -3	<u>2</u> -4	<u>3</u> -5
()	2. Practice Pattern Analysis	(37(<u>26</u> -1	<u>52</u> -2	<u>13</u> -3	<u>4</u> -4	<u>6</u> -5
()	3. The development of practice guidelines	(38(<u>28</u> -1	<u>50</u> -2	<u>15</u> -3	<u>5</u> -4	<u>1</u> -5
()	4. The reduction of fraud and abuse	(39(<u>37</u> -1	<u>46</u> -2	<u>15</u> -3	<u>1</u> -4	<u>*</u> -5

- M3a. How satisfied are you with the quality of the data currently available for (READ EACH ITEM) -- very satisfied, somewhat satisfied, not very satisfied, or not at all satisfied?

		Very	Somewhat	Not Very	Not	Not
		Satisfied	Satisfied	Satisfied	Satisfied	Sure
						At All
()	1. Outcomes research	(40(<u>4</u> -1	<u>45</u> -2	<u>32</u> -3	<u>11</u> -4	<u>9</u> -5
()	2. Practice Pattern Analysis	(41(<u>4</u> -1	<u>41</u> -2	<u>34</u> -3	<u>11</u> -4	<u>11</u> -5
()	3. The development of practice guidelines	(42(<u>5</u> -1	<u>45</u> -2	<u>33</u> -3	<u>10</u> -4	<u>7</u> -5
()	4. The reduction of fraud and abuse	(43(<u>5</u> -1	<u>39</u> -2	<u>36</u> -3	<u>13</u> -4	<u>7</u> -5

M3b. How satisfied are you with the quantity of the data currently available for (READ EACH ITEM) -- very satisfied, somewhat satisfied, not very satisfied, or not at all satisfied?

ROTATE -- START AT "X"		Very Satisfied	Somewhat Satisfied	Not Very Satisfied	Not Satisfied At All	Not Sure
()	1. Outcome research	44(<u>5</u> -1	<u>46</u> -2	<u>30</u> -3	<u>10</u> -4	<u>9</u> -5
()	2. Practice Pattern Analysis . .	45(<u>5</u> -1	<u>45</u> -2	<u>30</u> -3	<u>10</u> -4	<u>10</u> -5
()	3. The development of practice guidelines	46(<u>7</u> -1	<u>44</u> -2	<u>31</u> -3	<u>11</u> -4	<u>7</u> -5
()	4. The reduction of fraud and abuse	47(<u>5</u> -1	<u>43</u> -2	<u>32</u> -3	<u>11</u> -4	<u>8</u> -5

M4. How concerned do you think most Americans really are about threats to the confidentiality of their medical records -- do you think they are very concerned, somewhat concerned, not very concerned, or not at all concerned?

Very concerned.....(48(28 -1
Somewhat concerned.....43 -2
Not very concerned.....27 -3
Not at all concerned.....2 -4
Not sure.....* -5

M5. How serious a problem do you think the violation of medical records confidentiality is in America today -- very serious, somewhat serious, not very serious, or not at all serious?

Very serious.....(49(18 -1
Somewhat serious.....41 -2
Not very serious.....36 -3
Not at all serious.....4 -4
Not sure.....* -5

M6. Are you aware of any violations of the confidentiality of individuals' medical records from inside an organization that embarrassed or harmed the individual whose records were involved?

Yes.....(50(24 -1 (ASK Q.M7)
No.....76 -2 (SKIP TO Q.M11)
Not sure.....* -3

M7. Did these violations of medical records confidentiality occur involve manual records, computerized records, or both? (READ IF NECESSARY: Please think about the most recent violation you are aware of.)

Manual records.....(51(35 -1
Computerized records.....8 -2
Both.....50 -3
Not sure.....6 -4

M8. What kinds of medical records were involved? (READ IF NECESSARY: Please think about the most recent violation you are aware of.) (PROBE FOR SPECIFICS)

M9. Who revealed the information? DO NOT READ LIST -- MULTIPLE RECORD (READ IF NECESSARY: Please think about the most recent violation you are aware of.)

Physician.....	(52)	(10 -1)		
Hospital.....		15 -2		
Employer.....		3 -3		
Health insurer.....		10 -4		
Government employee.....		1 -5		
Federal Government employee.....		1 -6		
State Government employee.....		1 -7	Hospital/Lab	
Local Government employee.....		2 -8	employee/Nurse	22
Other (SPECIFY):				
		15 -9	Non-hospital	
Not sure.....	(53)	12 -0	employee: Doctor	16
			Ins. Office	

M10. How was the individual harmed? DO NOT READ LIST -- MULTIPLE RECORD (READ IF NECESSARY: Please think about the most recent violation you are aware of.)

Denied job.....	(54)	(6 -1)		
Denied promotion.....		3 -2	Lost job	7
Denied medical procedures.....		- -3	Denied coverage	6
Denied health insurance.....		12 -4	Damaged reputation	5
Denied reimbursement for claims.....		2 -5		
He/she was embarrassed.....		39 -6		
Other (SPECIFY):				
		24 -7		
Not sure.....		6 -8		

M11. In general, do you think the increased computerization of medical and health records could be managed to help strengthen the confidentiality of such records, or do you think computerization is almost certain to weaken confidentiality?

Could be managed to strengthen confidentiality...	(55)	(50 -1)
Almost certain to weaken confidentiality.....		45 -2
Not sure.....		5 -3

F. Demographics

(There is no F1-F3 in this version.)

56-59Z

F4. Finally, how would you describe your own personal political philosophy -- conservative, moderate, or liberal?

Conservative.....	(<u>37</u>	-1
Moderate.....		<u>46</u>	-2
Liberal.....		<u>16</u>	-3
Not sure.....		<u>1</u>	-4

(There is no F5-F9 in this version.)

61-65Z

That completes the interview. Thank you very much for your cooperation!

FROM OBSERVATION: Respondent Sex

Male.....	(66	<u>60</u>	-1
Female.....		<u>40</u>	-2

67-80Z

Time Ended: _____ A.M./P.M.



BOSTON PUBLIC LIBRARY



3 9999 05982 476 1

ISBN 0-16-046281-9



90000



9 780160 462818

