H.R. 3137: DATA NEEDS AND RELATED ISSUES FOR IMPLEMENTING HEALTH CARE REFORM

ARINGS

BEFORE THE

SUBCOMMITTEE ON CENSUS, STATISTICS AND POSTAL PERSONNEL

OF THE

COMMITTEE ON POST OFFICE AND CIVIL SERVICE HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

MARCH 2 AND 16, 1994

Serial No. 103–35

Printed for the use of the Committee on Post Office and Civil Service

U.S. GOVERNMENT PRINTING OFFICE
78–222 WASHINGTON : 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-044775-5

78-222 O – 94 – 1

H.R. 3137: DATA NEEDS AND RELATED ISSUES FOR IMPLEMENTING HEALTH CARE REFORM

HEARINGS

BEFORE THE

SUBCOMMITTEE ON CENSUS, STATISTICS AND POSTAL PERSONNEL

OF THE

COMMITTEE ON POST OFFICE AND CIVIL SERVICE HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

MARCH 2 AND 16, 1994

Serial No. 103–35

Printed for the use of the Committee on Post Office and Civil Service

U.S. GOVERNMENT PRINTING OFFICE

78–222 WASHINGTON : 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-044775-5

COMMITTEE ON POST OFFICE AND CIVIL SERVICE

WILLIAM L. CLAY, Missouri, *Chairman*

PATRICIA SCHROEDER, Colorado
FRANK McCLOSKEY, Indiana
GARY L. ACKERMAN, New York
THOMAS C. SAWYER, Ohio
PAUL E. KANJORSKI, Pennsylvania
ELEANOR HOLMES NORTON, District of Columbia
BARBARA-ROSE COLLINS, Michigan
LESLIE L. BYRNE, Virginia
MELVIN L. WATT, North Carolina
ALBERT RUSSELL WYNN, Maryland
GREG LAUGHLIN, Texas
SANFORD D. BISHOP, JR., Georgia
SHERROD BROWN, Ohio
ALCEE L. HASTINGS, Florida

JOHN T. MYERS, Indiana
BENJAMIN A. GILMAN, New York
DON YOUNG, Alaska
DAN BURTON, Indiana
CONSTANCE A. MORELLA, Maryland
THOMAS J. RIDGE, Pennsylvania
THOMAS E. PETRI, Wisconsin
SHERWOOD L. BOEHLERT, New York
(Vacancy)

GAIL E. WEISS, *Staff Director*
ROBERT E. LOCKHART, *General Counsel*
DORIS MOORE-GLENN, *Deputy Staff Director*
JOSEPH A. FISHER, *Minority Staff Director*

SUBCOMMITTEE ON CENSUS, STATISTICS AND POSTAL PERSONNEL

THOMAS C. SAWYER, Ohio, *Chairman*

FRANK McCLOSKEY, Indiana
ALBERT RUSSELL WYNN, Maryland
THOMAS E. PETRI, Wisconsin
THOMAS J. RIDGE, Pennsylvania

TERRIANN LOWENTHAL, *Subcommittee Staff Director*

CONTENTS

March 2, 1994

March 16, 1994

H.R. 3137: DATA NEEDS AND RELATED ISSUES FOR IMPLEMENTING HEALTH CARE REFORM

WEDNESDAY, MARCH 2, 1994

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CENSUS, STATISTICS
AND POSTAL PERSONNEL,
COMMITTEE ON POST OFFICE AND CIVIL SERVICE,
Washington, DC.

The subcommittee met pursuant to call, at 10:23 a.m., in room 311, Cannon House Office Building, the Hon. Thomas C. Sawyer (chairman of the subcommittee) presiding.

Members present: Representatives Sawyer and Petri.

Mr. SAWYER. Let me say good morning to everyone here today.

This represents the beginning in a series of hearings about the kind of national information system that will be fundamental to the success of any of the several forms of health care reform that is before the nation.

Each of these proposals is going to require a sophisticated information system that is far more extensive than any other data system in existence. It may ultimately contain some level of information about virtually every American who receives health care, which sooner or later becomes all of us.

There are some useful models. There is promising technology, but at least from a policy point of view, we are still really in our infancy in trying to decide what it is that we will need and how we will go about building it.

Any of the proposals that are before us still lack definition, dimensions, boundaries, and in some cases even clearly stated goals.

In the course of these hearings, I would like to ask a couple of questions. What do we want from the health care data system, and what is the appropriate federal role in establishing it?

In answering those questions, we first of all need to define what are our goals. Clearly, they include the importance of reducing paperwork burdens, detecting fraud, and providing for the timely and appropriate transmission of information among providers.

We hope that those data will be easily transferrable. If they are, then such an information system can become virtually the central nervous system of any form of health care reform, but it means that we have got to develop it with great care.

If we do, then such a system can provide us with valuable medical and demographic information that will not only serve individual beneficiaries, but inform a vast array of policy in this country. It has the potential to tell us about things like the effectiveness of treatments, incidence of disease or injury, and the relationship be-

tween health and other factors, both for individuals and broadly in the population. The uses are important.

But we need to pose a few other questions, like: what can an existing and emerging technology do and what can it not do? Who should control the information? Who should own it? Where should it repose? What combination of technology and policy will insure appropriate access where needed and insure preservation of confidentiality, a matter of importance to virtually every American?

The second concern we need to explore is the appropriate federal role. The technology already exists to replace a paper-based system, but there are barriers to the movement of that kind of information. They include lack of uniform delivery standards, multiple standards for some transactions and other kinds of transactions where no standards exist at all. We need to build a common language.

Privacy laws largely existing at the state level cover only, in most cases, paper-based information, leaving electronic data largely unprotected in some settings. Most third parties are not covered by state laws, and that kind of patchwork leaves many Americans concerned about what we might build, and if they thought about it, they ought to be concerned about what we have in place today.

The illusion of privacy is pervasive. Effective confidentiality may not exist to the degree that we think it does. So we have got to build a national policy to guard against inappropriate use of information in a patient's medical record.

And, finally, we need to decide who gets access and how. We need to provide for the effective management of health care and the information that drives it. Finally, we need to make sure that public health officials, social scientists, and medical researchers have the ability to make appropriate use of this enormously valuable tool without jeopardizing privacy.

Our March 16th hearing will focus on those kinds of policy issues based on research and statistical uses of information. Our witnesses today will do us a great service if they can point us in the direction of telling us what kind of system we can best hope to design and define more clearly the goals it should help us to achieve.

Tom.

Mr. PETRI. Thank you very much, Mr. Chairman.

You have outlined the catalog of concerns that we hope to make a little dent in and progress on. I would like to thank our witnesses and our colleague from Ohio, and others for taking the time to come and testify before this subcommittee.

There is no question that one of the major concerns that providers have, whether they are hospital administrators or doctors or employees in different aspects, as well as patients, is the complexity and almost impenetrability of much of the paper work and multiplication. We do not really quite know whether we are part of the problem, where the government is concerned, or part of the solution because I know in meeting with some of these people that private health insurance companies, which are often blamed for a lot, have worked out common forms in many cases and tried, not because they are good guys necessarily, although I am sure they are, but it is because they are efficient, and they can save money if they can make the flow of information go more smoothly.

But we have a large part of our economy now in health care. This is a health care session of Congress, and this is an important building block in making some real progress in providing better health care in our country.

So, again, thank you, and I look forward to your comments.

Mr. SAWYER. Thank you.

Let me join in that welcome to our colleague from Springfield, Ohio, Dave Hobson, who has shared service with me in the Ohio General Assembly. When he and I came together earlier this year to talk about how we might collaborate on this, I have to tell you that there was not a member of my delegation or, frankly, anywhere across the Congress that I would have been more pleased to work with than Dave.

I think the kind of partnership that we have had on this subcommittee and the kind of effort that we can put together here will represent a collaborative effort that will be compatible with virtually any direction that we might go this year in terms of making a start on building a health care system.

I particularly want to thank Dave for his effort in this regard, and I look forward to your testimony.

STATEMENT OF HON. DAVID L. HOBSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. HOBSON. Thank you, Mr. Chairman, and thank you, Mr. Ranking Member.

I truly appreciate this opportunity to discuss the bill, Mr. Chairman, that you and I introduced last October, H.R. 3137, the Health Care Information Modernization and Security Act.

I think that health care reform should be a bipartisan effort and partisan politics should be left out of this. I appreciate your working together with me on this bill.

Today's Washington Post highlighted one of the biggest problems with health care reform. People cannot support what they do not understand. Despite President Clinton's and the First Lady's good efforts, people say they do not understand their plan.

But people do understand the problems they face every day dealing with our current health care system. Just ask the person on Medicare, like my mom, who must suffer the anxiety of filling out confusing forms. She actually has a person that comes in and fills out a lot of her forms because, first of all, she has a problem with her sight, but also because of the proliferation of forms. There is a lot of trauma and anxiety that results from that, especially if a mistake is made. Older people really have a problem with that.

Take also the physician who is forced to spend less time with patients and more time completing paperwork. President Clinton was correct when he said a hospital ought to be a house of healing, not a monument to paperwork and bureaucracy.

There are significant financial costs that impact everyone, as well. We pay for the paperwork burden in higher insurance premiums and higher medical bills that consume as much as ten cents out of every health care dollar.

People want solutions that address these problems. An electronic care data network, in my opinion, would do just that, but there are not uniform standards to allow this technology to fully develop. To

make this work a hospital, for example, in Ohio must be able to communicate with an insurance company in Chicago, which then must be able to contact Medicare in Baltimore. Today these providers often speak in a different electronic language which is not compatible.

In H.R. 3137 we remove the barriers that have slowed the development of an electronic health care data network. It adopts standard forms for health care data and assures patient privacy and confidentiality of medical records.

H.R. 3137 was developed over several years in an open, cooperative effort among technical experts, agency officials, legislators, and industry representatives, some of whom are here today and will elaborate on the details and the benefits of this bill.

The political support for H.R. 3137 is bipartisan and bicameral. Senator Bond and Senator Reigle, Congressman Sawyer and myself are the primary sponsors in both houses.

H.R. 3137 was intentionally written to complement comprehensive reform. Each of the comprehensive reform proposals, the Clinton proposal, Cooper, Chafee, McDermott, and the House Republican plan, sketch an outline for reform. We simply attempt to fill in the details.

I want to discuss a few of those details. H.R. 3137 establishes a health care data panel to adopt uniform data standards. The panel includes government officials and private sector experts who represent different professions, geographic areas, federal and state government, health programs, applicable standard setting groups, and consumers of health care services.

The panel develops data standards so providers, insurers, and others can communicate in the same standard electronic language. When possible, the data standards must reflect existing, widely adopted standards.

The data standards are implemented according to an aggressive time table. Within nine months after enactment of this bill, financial and administrative transactions must be standardized. Within 12 months, an initial inquiry indicator data set must be standardized, and within two years, a comprehensive clinical data set must be standardized.

In the case of the more complicated clinical data set, there is a two-year grace period for compliance. There are waivers for small and rural hospitals who may have difficulty in acquiring the technology early.

H.R. 3137 outlines specific principles to guide the development of patient privacy and confidentiality of medical information. The House Committee on Government Operations is working on detailed privacy standards. We will make sure that our bill is consistent with their efforts.

The benefits of reducing excessive paperwork and administrative waste in our health care system are significant. Conservative estimates indicate an electronic health care data network would save $4 billion annually in administrative costs. It would save $20 billion annually by providing medical researchers, physicians, and hospitals with the clinical data they need to reduce unnecessary and costly medical procedures, and by reducing health fraud, it could save as much as $150 billion annually.

These savings are significant, but in achieving these savings and in computerizing all of these various health transactions, we also create a system capable of much more than just paperwork simplification.

Today fragmented information makes it difficult to reform our health care system. H.R. 3137 creates the information infrastructure necessary to provide the comprehensive data needed to enact effective reform. As I mentioned, our plan is the foundation for comprehensive reform. It is consistent with insurance reform, managed competition, and single payer.

Today information on costs and quality among hospitals and benefit plans is not available to consumers. We create a system that provides the data consumers need to compare the value of insurance plans and health services. Our plan allows consumers to make the smart choices that are necessary to make competition work.

Today information on the effectiveness of medical procedures is unavailable or scattered among providers in unusable form. We create the tools needed for outcomes research to improve the quality of care. We provide researchers, physicians, and hospitals with the clinical data they need to reduce unnecessary medical procedures.

And today the confusing, disjointed paperwork system provides cover for the consumer or provider who wants to cheat the system. We make it possible to expose fraud in ways that are impossible to do under the paperwork system that we have today.

I recall a bill I did in the state legislature. We had people who committed fraud whom we would throw out of the system, and they would change their name and come back in the system. We tried to reduce fraud then, and now will do it nationwide through a computer network.

Mr. Chairman, thank you again for convening this panel and for your work to continually improve H.R. 3137. Your understanding of the technical aspects of data collection and transfer have been invaluable in this process.

Also I want to thank everyone who is testifying here today. What we propose as legislators is a simple outline. It is industry groups and health care providers that will fill in the details and make these systems work for all Americans.

Your input and involvement is vital to the success of this effort. I look forward to their testimony, and I will be glad to respond to your questions, Mr. Chairman and Mr. Ranking Member.

[The prepared statement of Hon. David L. Hobson follows:]

PREPARED STATEMENT OF HON. DAVID L. HOBSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

INTRODUCTION

Mr. Chairman, I appreciate this opportunity to discuss the bill you and I introduced last October -- H.R. 3137, the Health Care Information Modernization and Security Act.

As you know, the paperwork burden in our health care system impacts everyone. We pay for this burden in higher insurance premiums and medical bills that consume as much as 10 cents of every health care dollar.

But the cost is greater than dollars. Just ask the person on Medicare who must suffer the anxiety of filling out confusing forms, or the physician who is forced to spend less time with patients and more time completing paperwork. President Clinton was correct when he said, "A hospital ought to be a house of healing, not a monument to paperwork and bureaucracy."

The technology exists today to move away from a paperwork system and toward an electronic health care data network. But there are no uniform standards to allow this technology to fully develop. To make this work, a hospital in Ohio must be able to communicate with an insurance company in Chicago, which then must be able to contact Medicare in Baltimore. Today, these providers often speak a different electronic language.

BACKGROUND

H.R. 3137 removes the barriers that have slowed the development of an electronic health care data network. It adopts standards for health care data and ensures patient privacy and confidentiality of medical records.

H.R. 3137 was developed over several years in an open, cooperative effort among technical experts, agency officials, legislators and industry representatives -- some of whom are here today and will elaborate on the details and benefits of the bill. The political support for H.R. 3137 is bipartisan and bicameral -- Senator Bond, Senator Reigle, Congressman Sawyer and myself are the primary sponsors.

H.R. 3137 was intentionally written to complement comprehensive reform. Each of the comprehensive reform proposals -- Clinton, Cooper, Chafee, McDermott, House GOP -- sketch an outline for administrative reform. We simply fill in the details.

HEALTH CARE DATA PANEL

I want to discuss a few of those details. H.R. 3137 establishes a Health Care Data Panel to adopt uniform data standards. The Panel includes government officials and private sector experts who represent different professions, geographic areas, federal or state government health programs, applicable standard-setting groups, and consumers of health care services.

DATA STANDARDS

The Panel develops data standards so providers, insurers and others can communicate in the same, standard electronic language. When possible, the data standards must reflect existing, widely-adopted standards.

The data standards are implemented according to an aggressive timetable. Within nine months after enactment of this bill, financial and administrative transactions must be standardized; within twelve months, an initial quality indicator data set must be standardized; and within two years, a comprehensive clinical data set must be standardized. In the case of the more complicated clinical data set, there is a two-year grace period for compliance. There are waivers for small and rural hospitals.

PRIVACY AND CONFIDENTIALITY REQUIREMENTS

H.R. 3137 outlines specific principles to guide the development of patient privacy and confidentiality of medical information. The House Committee on Government Operations is working on detailed privacy standards. We will make sure that our bill is consistent with their efforts.

IMPACT

The benefits of reducing excessive paperwork and administrative waste in our health care system are significant. Conservative estimates indicate an electronic health care data network would save 4 billion dollars annually in administrative costs. It would save 20 billion dollars annually by providing medical researchers, physicians, and hospitals with the clinical data they need to reduce unnecessary and costly medical procedures. And by reducing health fraud it could save as much as 150 billion dollars annually.

These savings are significant, but in achieving these savings -- in computerizing all of these various health transactions -- we also create a system capable of much more than just paperwork simplification.

Today, fragmented information makes it difficult to reform our health care system. H.R. 3137 creates the information infrastructure necessary to provide the comprehensive data needed to enact effective reform. As I mentioned, our plan is the foundation for comprehensive reform. It is consistent with insurance reform, managed competition, and single-payer.

Today, information on cost and quality among hospitals and benefit plans is not available to consumers. We create a system that provides the data consumers need to compare the value of insurance plans and health services. Our plan allows consumers to make the smart choices that are necessary to make competition work.

Today, information on the effectiveness of medical procedures is unavailable or scattered among providers in an unusable form. We create the tools needed for outcomes research to improve the quality of care. We provide researchers, physicians, and hospitals with the clinical data they need to reduce unnecessary medical procedures.

And today, the confusing, disjointed paperwork system provides cover for the consumer or provider who wants to cheat the system. We make it possible to expose fraud in ways that are impossible to do under the paperwork system we have today.

CONCLUSION

Mr. Chairman, thank you again for convening this panel, and for your work to continually improve H.R. 3137. Your understanding of the technical aspects of data collection and transfer have been invaluable to this process.

Also, I want to thank everyone who is testifying here today. What we propose as legislators is a simple outline -- it is industry groups and health care providers that will fill in the details and make these systems work. Your input and involvement is vital to the success of this effort. I look forward to your testimony.

Mr. SAWYER. Thank you very much, Dave.

The kind of work that you have done not just here, but in the Ohio senate really has earned for you a reputation that you richly deserve, and it is a pleasure to work with you on this.

Tom, do you have any questions?

Mr. PETRI. I have a comment. I would like again to commend you for this. It occurs to me that back when the Industrial Revolution made its sweep across our economy in the 1920's, a fellow named Herbert Hoover distinguished himself as Commerce Secretary by convening industry by industry panels and working very, very hard to develop standard parts, standard screws and nuts and bolts and all of these sorts of things because each company was having their own standards, you know, so that there was some small advantage, but overall the economy lost out of that if Ford used different standards than Chrysler, and so on.

So here, again, we are doing something that sounds new and exciting, but it really is a logical step forward from where we are now in the data revolution that we have just been going through, and I certainly commend you for that and hope that industry and others get on board and look at what is already being done and build on it so that we can make progress fast rather than slowly in this important effort.

Mr. HOBSON. I appreciate that because this is the beginning of the nuts and bolts, because as we look at the health care changes that are coming, we have to be prepared for changes in the information age. We are doing that in other pieces of legislation, but we need to do that here as well. And we need to keep the private sector, as well as the public sector, involved so that they better interface in this system.

I think a lot of us are concerned that we do not take one bureaucracy, shift it to another bureaucracy, and then create different kinds of problems or worse problems than we have now. No matter what plan you are talking about nor what industry group you are talking about. There seems to be a sense of understanding that we need to move in these directions just as you have discussed.

So I think we are doing some pioneering. Before we can reach the end, there will be some problems as we work through this. That is one of the reasons I am glad that you are here and the Chairman, because you both have a background in these areas that I think is going to be very important in working with these groups.

You know, sometimes we all get caught up in partisanship in some of this stuff, but that does not have to happen in this area at all.

Mr. SAWYER. Let me suggest without objection that we ask Dave to join us so he can take part in the hearing, if I can get Tom not to suggest somehow that we have got a screw loose on this thing.

Mr. HOBSON. Thank you very much. I would like to stay for a few minutes, if I may, to hear some of the industry representatives. I do have to go over and meet Mr. Kasich on some budget items, but this should help in the budget in the future.

Mr. PETRI. Just one question. The National Academy, have they been involved in this at all? Sometimes Congress or the administration will turn to the National Engineering Academy or others, and they do a lot of important work in this type of area for us.

Mr. HOBSON. We are very desirous of having the input of all groups into this because this is going to be a major revolution in the transfer of information, and so we want to get everybody to have their input.

Mr. SAWYER. Good. Why don't you come join us?

Our second panel this morning will consist of Kathleen A. Frawley, Director of the Washington office of the American Health Information Management Association; Warren Hern, who is the Secretary of the Healthcare Financial Management Association; and Mark Epstein, who is the Executive Director of the National Association of Health Data Organizations.

Thank you for being with us this morning. We look forward to your testimony. Let me emphasize that the full text of your testimony will be included in the record, and you should feel free to summarize, to focus, to emphasize, to elevate whatever parts of your testimony you feel best can share your message with us this morning.

Why don't we simply proceed in the order in which you were introduced? Ms. Frawley.

STATEMENT OF KATHLEEN A. FRAWLEY, DIRECTOR, WASHINGTON OFFICE, AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION; WARREN HERN, SECRETARY, BOARD OF DIRECTORS, HEALTHCARE FINANCIAL MANAGEMENT ASSOCIATION; AND MARK H. EPSTEIN, EXECUTIVE DIRECTOR, NATIONAL ASSOCIATION OF HEALTH DATA ORGANIZATIONS

Ms. FRAWLEY. Mr. Chairman, thank you.

My name is Kathleen A. Frawley, and I am Director of the Washington, D.C., office of the American Health Information Management Association.

AHIMA appreciates this opportunity to appear before the subcommittee to present its views on the essential components of an effective information system for health care reform.

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.

In April 1991, the Institute of Medicine released the report, The Computer Based Patient Record, an Essential Technology for Health Care. This report recommended the adoption of computer based patient records by the year 2000 and the formation of a nationwide health information network.

The IOM report clearly identified that the practice of health care in this country is seriously hampered by the lack of tools to efficiently access and manage clinical information. As health care reform is addressed, it becomes increasingly clear that more complete and accurate information is needed for more effective delivery of health care, improving the quality of care, evaluating the cost of health care, and the administrative costs associated with it, supporting public health and research activities, improving the ability of consumers to make informed choices, and managing and containing costs of health care.

To meet those information requirements, the Nation must move towards a health information infrastructure which will support computer based patient record systems that capture clinical information, integrate it with clinical decision, support, and knowledge bases, and make it available for all legitimate users.

Because health information remains largely uncomputerized and unintegrated, patient information is often inaccessible at the time health care decisions are made. Highly trained health care professionals spend valuable time looking for records, contacting each other to obtain basic information, struggling to decipher handwritten entries, or repeating tests because previous results could not be found or obtained quickly enough.

National studies have estimated that health care providers spend on average approximately 40 percent of their time on paperwork. External users of health information, such as payers, researchers, Governmental agencies, and others, must depend on a limited set of data that is often not transmitted electronically or sought through volumes of records for key information about a health care encounter.

There are a number of benefits that can be achieved through widespread use of computer based patient record systems. Health care providers would have more complete information about the patient instantly and easily. Care would be improved through the ability to access knowledge databases and on-line expert systems. Information systems would reduce the enormous paperwork burden that providers currently experience. Aggregate data from these records would enable better research.

One of the major prerequisites to the appropriate implementation of a computer based patient record is development of standards to insure the uniform electronic recording and transmission of clinical information. Standards are necessary to link information systems across provider settings and are essential to achieve the concept of a longitudinal health record and to contribute to health planning and research.

The development of the national 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. In order to address the need for Federal legislation, the American Health Information Management Association drafted model language in February and March of 1993, with input from our members, members of the Computer Based Patient Record Institute Work Group on Confidentiality, and Privacy and Legislation, and individuals from other professional associations.

This model language was presented to members of the White House Task Force on Health Care Reform in April of 1993. There are a number of key provisions in our model language which we believe are essential elements of any legislation to govern the collection, use and disclosure of health care information.

A complete copy of our model language has been shared with staff to the subcommittee and has been outlined in our written testimony.

It is critical that as we begin to build the information infrastructure that is necessary to improve patient care and reduce the administrative costs of our health care system, AHIMA offers the following recommendations:

Number one, the computer based patient records should become the standard for all medical and other records related to patient care.

Number two, Federal legislation should be enacted to insure the privacy and confidentiality of computer based health information. AHIMA's model legislation should be considered in fully developing the specific provisions outlined in H.R. 3137.

Number three, third party payers and health care providers should adopt the electronic format developed by ANSI's Insurance Subcommittee of the Accredited Standards Committee X–12 for Claims Processing.

And, number four, uniform claims form and data set for electronic transmission of health coverage information and billing data should be implemented for use by all third party payers and health care providers.

Many of these recommendations are currently addressed in H.R. 3137, and AHIMA is pleased to support this bill. We would like to congratulate you, Mr. Chairman and Congressman Hobson, for your efforts to initiate a framework for an effective information system.

Thank you for the opportunity to present our views, and we look forward to working with the subcommittee on these issues.

[The prepared statement of Ms. Frawley follows:]

PREPARED STATEMENT OF KATHLEEN A. FRAWLEY, DIRECTOR, WASHINGTON OFFICE, AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION

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 essential components of an effective information system for heathcare reform.

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.

In April 1991, the Institute of Medicine released the report, "The Computer-Based Patient Record: An Essential Technology for Health Care". This report recommended the adoption of computer-based patient records by the year 2000 and the formation of a nationwide health information network. The Computer-Based Patient Record Institute (CPRI) was established in 1992 to facilitate the attainment of these objectives. CPRI is a non-profit organization comprised of provider organizations, other groups and individuals representing the diverse interests of health care. AHIMA has been an active force in the formation of CPRI and provides leadership on the Board of Directors and in the various workgroups.

The IOM report clearly identified that the practice of health care in this country is seriously hampered by the lack of tools to efficiently access and manage clinical information. As healthcare reform is addressed, it becomes increasingly clear that more complete and accurate information is essential for

- o more effective delivery of health care,
- o improving the quality of care,
- o evaluating the cost of health care and the administrative costs associated with it,
- o supporting public health and research activities,
- o improving the ability of consumers to make informed choices and
- o managing and containing costs of health care.

To meet those information requirements, the nation must move towards a health information infrastructure which will support computer-based patient record systems that capture clinical information, integrate it with clinical decision support and knowledge bases, and make it available for all legitimate users.

Because health information remains largely uncomputerized and unintegrated, patient information is often inaccessible at the time health care decisions are made. Highly trained health care professionals spend valuable time looking for records, contacting each other to obtain basic information, struggling to decipher handwritten entries or repeating tests because previous

results could not be found or obtained quickly enough. National studies have estimated that health care providers spend on average approximately 40 percent of their time on paperwork.

External users of health information, such as payors, researchers, governmental agencies and others must depend on a limited set of data that often is not transmitted electronically or sort through volumes of records for key information about an encounter.

There are a number of benefits which can be achieved through widespread use of computer-based patient record systems. Health care providers would have more complete information about the patient instantly and easily. Care would be improved through the ability to access knowledge databases and online expert systems. Information systems would reduce the enormous paperwork burden that providers currently experience. Aggregated data from medical records these will enable better research.

One of the major prerequisites to the appropriate implementation of the computer-based patient record is development of standards to ensure uniform electronic recording and transmission of clinical information. Standards are necessary to link information systems across provider settings and are essential to achieve the concept of a longitudinal health record and to contribute to health planning and research.

In November 1991, the Secretary of Health and Human Services convened a forum of health care leaders to identify ways to reduce the administrative costs of healthcare. The Workgroup on Electronic Data Interchange (WEDI) was formed to address issues regarding claims processing. AHIMA has participated on the WEDI Steering Committee since its inception. AHIMA supports the findings of WEDI and recommends the development of a standardized electronic health insurance claims and payment system.

NEED FOR FEDERAL LEGISLATION

In order to ensure the widespread use of information technology in healthcare, federal legislation is needed to protect the confidentiality of health information.

The recently released Office of Technology (OTA) report, Protecting Privacy in Computerized Medical Information, 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. Senator Patrick Leahy (D-VT) and Representative Pete Stark (D-CA) and several 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.

Currently, there is little uniformity among state licensure laws and regulations regarding confidentiality of health information. It has been recognized that there is a need for more uniformity among the 50 states. In recent years, the National

Conference of Commissioners on Uniform State Laws developed the Uniform Health Care Information Act in an attempt to stimulate uniformity among states on health care information management issues. Presently, only two states, Montana and Washington, have enacted this model legislation. Clearly, efforts must be directed toward developing national standards on privacy and confidentiality.

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.

H. R. 3137, the Health Care Information Modernization and Security Act of 1993 contains specific provisions to address privacy and to ensure the confidentiality of information in the data interchange system.

AHIMA'S POSITION

In order to address the need for federal legislation, the

American Health Information Management Association (AHIMA) drafted model language in February and March of 1993 with input from AHIMA members, members of the Computer-Based Patient Record Institute Workgroup on Confidentiality, Privacy and Legislation and individuals from other professional associations.

This model language was presented to members of The White House Task Force on Healthcare Reform on April 29, 1993 and was also included in the OTA report. There are a number of key provisions in AHIMA's model language which we believe must be essential elements of any legislation to govern the collection, use and disclosure of health care records. These include:

- **Disclosure** -- No person other than the patient or the patient's representative may disclose health care information to any other person without the patient's authorization, except as authorized.

  No person may disclose health care information except in accordance with the terms of the patient's authorization.

  The provisions apply both to disclosures of health care information and to redisclosures of health care information by a person to whom health care information is disclosed.

- **Record of Disclosure** -- Each person maintaining health care information shall maintain a record of all external disclosures of health care information made by such person concerning each patient, and such record shall become part of the health care information concerning each patient. The record of each disclosure shall include the name, address and institutional affiliation, if any, of the person to whom the health care information is disclosed, the date and purpose of the disclosure and, to the extent practicable, a description of the information disclosed.

- **Patient's Authorization; Requirements for Validity** -- To be valid, a patient's authorization must --

1) Identify the patient;
2) Generally describe the health care information to be disclosed;
3) Identify the person to whom the health care information is to be disclosed;
4) Describe the purpose of this disclosure;
5) Limit the length of time the patient's authorization will remain valid;
6) Be given by one of the following means --
   a) In writing, dated and signed by the patient or the patient's representative; or
   b) In electronic form, dated and authenticated

by the patient or the patient's representative using a unique identifier.

The AHIMA model also includes the following principles of fair information practices:

- **Patient's right to know** -- The patient or the patient's representative has the right to know that health care information concerning the patient is maintained by any person and to know for what purpose the health care information is used.

- **Restrictions on collection** -- Health care information concerning a patient must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected.

- **Collection and use only for lawful purpose** -- Health care information must be collected and used only for a necessary and lawful purpose.

- **Notification to patient** -- Each person maintaining health care information must prepare a formal, written statement of the fair information practices observed by such person. Each patient who provides health care information directly to a person maintaining health care information should receive a copy of the statement

of a person's fair information practices and should receive an explanation of such fair information practices upon request.

- **Restriction on use for other purposes** -- Health care information may not be used for any purpose beyond the purpose for which the health care information is collected, except as otherwise provided.

- **Right to access** -- The patient or the patient's representative may have access to health care information concerning the patient, has the right to have a copy of such health care information made after payment of a reasonable charge, and, further, has the right to have a notation made with or in such health care information of any amendment or correction of such health care information requested by the patient or patient representative.

- **Required safeguards** -- Any person maintaining, using or disseminating health care information shall implement reasonable safeguards for the security of the health care information and its storage, processing and transmission, whether in electronic or other form.

- **Additional protections** -- Methods to ensure the accuracy, reliability, relevance, completeness and timeliness

of the health care information should be instituted. If advisable, additional safeguards for highly sensitive health care information should be provided.

The AHIMA model language also contains provisions for civil and criminal penalties to protect against unauthorized use or disclosure.

CONCLUSION

It is critical that we begin to build the information infrastructure that is necessary to improve patient care and reduce the administrative costs of our healthcare system. If Congress procedes properly, thims important effort to build an information infrastructure can be achieved without undo risk to the privacy and confidentiality of health information. AHIMA offers the following recommendations:

o The computer-based patient record (CPR) should become the standard for all medical and other records related to patient care.

o Federal legislation should be enacted to ensure the privacy and confidentiality of computer-based health information. AHIMA's model legislation should be considered in developing the specific provisions as outlined in H. R. 3137.

o Third party payors and healthcare providers should adopt the electronic format developed by ANSI's Insurance

Subcommittee of the Accredited Standards Committee X12 for claims processing.

o A uniform claims form and data set for electronic transmission of health coverage information and billing data should be implemented for use by all third party payors and healthcare providers.

Thank you for the opportunity to present our views. We look forward to working with the Subcommittee on these important issues.

Mr. SAWYER. Thank you very much for your testimony. We will return for questions in a moment.

I just want to compliment you on not only the concision of your oral statement, but the thoroughness of your written statement. I just really want to reassure you that we value that written part of the record as well.

Ms. FRAWLEY. Thank you very much.

Mr. SAWYER. Mr. Hern.

Mr. HERN. Good morning, Mr. Chairman and Congressman Hobson.

My name is Warren Hern, and I am here today representing Healthcare Financial Management Association. I am a Fellow of the organization and have been a member for 16 years, and I currently serve on the Board of Directors and am Secretary.

I am also Senior Vice President and Chief Financial Officer for Park Ridge Health System, which is located in Rochester, New York. Park Ridge Health System provides a full array of services, including a hospital, several skilled nursing facilities, senior housing, child care, among other services.

HFMA represents over 31,000 professionals involved in the financial management of various types of health care institutions. This includes hospitals, clinics, managed care providers, physicians' offices, as well as insurers, and other health care financial professionals.

On behalf of these individuals, Mr. Chairman, I appreciate the opportunity to present our views on health care administrator's simplification. I would also like to thank you for taking such a prominent role in this issue.

From a professional perspective, I can tell you that administrative simplification is needed, and it is needed now. I cannot begin to describe the difficult choices I must make when attempting to maintain the balance between sound financial planning and quality health care delivery. Often the decisions boil down to whether new clinical staff could be hired to meet the health care needs of our patients or whether more clerical staff are needed to move the mountains of paperwork, make the hundreds of phone calls, and decipher the never ending iteration of billing claim forms.

HFMA's membership is very diverse both in geography and professional affiliation. This puts us in a unique position of being able to identify problems associated with health care claims and patient accounting and develop solutions to those problems.

HFMA determined several years ago the need for uniformity and simplification and in working closely with our members, developed a detailed plan to achieve that goal. For the past two years we have presented our plan to Congress and the administration.

We recently revisited our proposal and found the approach is still feasible, practical and cost effective. The fundamentals of administrative simplification are to streamline and standardize health care business transactions. Our written statement provides a detailed analysis of how this can be achieved.

It also provides the details of seven principles HFMA believes should be used when developing a plan to implement simplification. Very briefly, these principles are: total industry compliance; use of an industry commission reporting to Congress; the mandated

use of electronic transmissions; defined basic core transactions, such as enrollment, eligibility and claims; a national coordinated database; confidentiality and privacy protection with use of uniform identifiers; and, lastly, strategic time tables that are realistic and constructive to the transition process.

Mr. Chairman, we urge you and the members of your subcommittee to use these principles when deliberating this issue.

We are please that administrative simplification is so prominent in many health care reform proposals pending in Congress, including the President's Health Security Act. We have worked closely with you, Mr. Chairman, your staff, and other members of the House and Senate, most notably Representative Hobson and Senators Bond, Reigle, and Burns.

We appreciate all that you have done to draft and introduce the Health Care Information, Modernization and Security Act of 1993. Our written statement includes an analysis of that bill and the administrative simplification provisions included in other health care reform proposals.

Mr. Chairman, administrative simplification can and should be enacted with or without overall health care reform. Last spring we contracted with Lewin VHI to study the projected savings of administrative simplification. That study concluded that an automated uniform system of reporting health care financial data can save $3 to $6 billion per year.

We recognize the need for comprehensive health care reform. However, we remain convinced that certain key elements of health care reform can be enacted quickly. Administrative simplification is one of those key elements.

On behalf of HFMA, I appreciate this opportunity to appear before you today. We are available to be of technical assistance to you and are pleased to offer expert guidance as you make decisions.

Thank you.

[The prepared statement of Mr. Hern follows:]

PREPARED STATEMENT OF WARREN HERN, SECRETARY, BOARD OF DIRECTORS,
HEALTHCARE FINANCIAL MANAGEMENT ASSOCIATION

SUMMARY

The Healthcare Financial Management Association supports the immediate implementation of a system which would:

- Provide universal electronic processes for healthcare enrollment, eligibility, coordination of benefits, first report of injury, billing, claims follow-up and payment and remittance to be used by *all* healthcare providers and third-party payers, while allowing alternative mechanisms for smaller providers and employers.

- Form an independent healthcare administrative commission, reporting to Congress, and comprising representatives from the industry and the government. The commission would recommend to the Executive Branch uniform standards that would permit the creation of the universal claims process system; and would provide Congress an ongoing assessment of the system.

These two primary initiatives would:

- Apply to all private and government sponsored healthcare benefit plans.

- Assure the development of an electronic system that provides a universal administrative process for the healthcare industry.

- Provide rules and information transfer mechanisms to facilitate coordination of benefits and the Medicare Secondary Payer program.

- Implement a system that will standardize the use of nationally acceptable electronic transmission standards.

- Allow healthcare providers (including rural and small providers), payers, and sponsors, unable to use the electronic transmission systems, to alternatively use clearinghouses.

- Pre-empt any state or local laws addressing hard copy documentation of medical, healthcare benefit plan records or data, or confidentiality.

- Provide that any changes to the current system are implemented within a realistic strategic timetable.

INTRODUCTION

Good morning, Mr. Chairman and members of the Subcommittee. My name is Warren Hern, and I am here today representing the Healthcare Financial Management Association (HFMA). I am a fellow of the organization, and have been a member of the organization for 16 years. I currently serve on its Board of Directors as Secretary. I am also the senior vice president and chief financial officer of Park Ridge Health System, Inc., which is located in Rochester, New York. Park Ridge Health System is a vertically integrated organization which includes a hospital, three skilled nursing facilities, a charitable foundation, mental health and chemical dependency centers, senior housing, and a child care center.

HFMA represents more than 31,500 professionals involved in the financial management of various types of healthcare institutions, including hospitals and clinics, managed care providers, public accountants, consultants, insurance companies, governmental agencies and other organizations. Given the geographic and professional diversity of its members, HFMA is in a unique position to identify the problems associated with the current healthcare claims and patient accounting processes. Based on our analysis of the current healthcare administrative system, we have determined there is a definite need for uniformity and simplification. Moreover, administrative simplification can and should begin now. After in-depth consultation with our members and others, we developed a detailed plan to achieve this goal. On behalf of these individuals, I appreciate the opportunity to present our views on healthcare administrative costs and to offer an approach to simplifying the processes associated with these costs.

Based on my professional experience, I would like to stress that administrative simplification is needed, and that it is needed now. As a chief financial officer, my responsibilities include overall financial planning and operations, information systems and admitting procedures. My position compels me to make tough decisions, careful to maintain the balance between sound financial planning and quality healthcare delivery. Often the decisions boiled down to whether new clinical staff could be hired to meet the healthcare needs of our patients, or whether more clerical personnel needed to be hired to move the mountains of paperwork, make the hundreds of phone calls and decipher the never ending iterations of billing claim forms.

I am proud to be part of a dedicated, professional society of financial management executives that is tackling this critical dilemma; a dilemma that wastes billions of dollars each year. HFMA believes strongly that an immediate implementation of administrative simplification is needed now, and would be compatible with whatever system of healthcare reform is passed.

HFMA PROPOSAL FOR HEALTHCARE ADMINISTRATIVE SIMPLIFICATION AND UNIFORMITY

Mr. Chairman, over the past two years we have had the opportunity to present HFMA's proposed administrative simplification process to Congress and the Administration. That proposal would simplify the current healthcare administrative processes through the mandated use of various electronic mechanisms for all participants in the healthcare delivery system. It has been reviewed by healthcare financial managers and others involved with these processes. These professionals have confirmed that the concepts contained in our proposal are feasible, practical and will meet the goals of Congress, the Administration, the healthcare community, and most importantly, the consumer.

Very briefly, the fundamental goals of administrative simplification are to simplify and standardize the healthcare administrative functions of enrollment, eligibility, coordination of benefits, billing, and payment for all healthcare providers and third-party payers. This can be accomplished through two primary initiatives:

- Provide universal electronic processes for healthcare enrollment, eligibility, coordination of benefits, first report of injury, billing, claims follow-up and payment and remittance to be used by *all* healthcare providers and third-party payers. Alternative mechanisms would be allowed for smaller providers and employers.

- Form an independent healthcare administrative commission, reporting to Congress, and comprising representatives from the industry and the government. This commission would recommend to the Executive Branch uniform standards for the creation of the universal claims process system; and would provide Congress an ongoing assessment of the system.

These two primary initiatives would:

- Apply to all private and government sponsored healthcare benefit plans.

- Assure the development of an electronic system that provides a universal administrative process for the healthcare industry.

- Provide rules and information transfer mechanisms to facilitate coordination of benefits and the Medicare Secondary Payer program.

- Implement a system that will standardize the use of nationally acceptable electronic transmission standards.

- Allow healthcare providers (including rural and small providers), payers, and sponsors unable to use the electronic transmission systems to alternatively use clearinghouses.

- Pre-empt any state or local laws addressing hard copy documentation of medical, healthcare benefit plan records or data, or confidentiality.

- Establish universal identification numbers for all participants in the healthcare delivery system.

- Provide that any changes to the current system are implemented within a realistic strategic timetable.

HFMA's concept can be broken down according to the following seven principles:

I. Total Industry Compliance

A. Administrative simplification will not be achieved unless *all* members of the healthcare community are mandated to participate.

1. This includes governmental and private sponsors (employers, unions, government bodies), providers, payers/administrators, vendors, suppliers, etc.

B. Any new programs, systems, mechanisms, etc., established to achieve simplification must be continually reviewed to ensure that the goals are being achieved without increasing costs.

II. Use of an Industry Commission Reporting to Congress

A. To ensure total involvement by the healthcare community, there must be an industry based commission to set appropriate standards.

1. To avoid domination by any one segment of the community, the commission should report to Congress.

B. Commission members should include healthcare financial managers, healthcare practitioners, and third-party payers, including government representatives.

III. Electronic Transactions

A. To direct the healthcare community toward the same level of sophistication as other U.S. industries, administrative simplification should mandate only electronic solutions.

B. The overall electronic mechanism should use existing data interface standards, such as those standards devised by the Insurance Subcommittee of the Accredited Standards Committee X12 of the American National Standards Institute (ANSI).

C. Clearinghouses and value added networks (VANs) are appropriate mechanisms to provide assistance to those members of the healthcare community that are unable to directly interface electronically.

IV. Core Transactions

A. The Commission should *initially* address the following "core transactions:" enrollment, eligibility, billing/claims, coordination of benefits, billing follow-up, first report of injury, and payment/remittance.

B. Uniformity or administrative simplification cannot occur without uniform data definitions, data sets with *maximum approved data*, and integration of such definitions and uniformity requirements.

V. Data Maintenance

A. The Federal government should maintain a central or shared data base.

1. Government control assures access by all, and appropriate data security and privacy controls.

VI. Confidentiality, Privacy, and Pre-emption of State and Federal Laws Governing Electronic Data with Uniform Identifiers

A. To achieve total uniformity, existing state requirements addressing privacy, confidentiality, and electronic data standards should be pre-empted by Federal law.

B. There must be uniform identifiers for most participants in the healthcare delivery system.

VII. Strategic Timetables

A. In recognition of limitations/difficulties in implementing administrative simplification and uniformity, any legislation must include a reasonable and strategic timetable to ensure against increased costs and/or diminished efficiency.

1. The industry based commission will be best able to make such implementation plans and, therefore, timetables for implementation should not be legislated.

Mr. Chairman, HFMA strongly supports these principles. We urge you and the members of your Subcommittee to consider these principles when deliberating possible solutions to the current problems with the healthcare administrative process.

Mr. Chairman, administrative simplification can and should be enacted now, with or without overall healthcare reform. While a total overhaul of the healthcare system may be preferable, enacting a comprehensive reform package may take longer than anticipated. Administrative simplification, in and of itself, will result in substantial savings to the healthcare system, thereby increasing the availability of public and private funds that can then be directed to other essential areas of the healthcare delivery system.

DISCUSSION OF THE PROBLEM

For 25 years, healthcare providers and third-party payers have worked toward administrative uniformity. While the joint effort is essential, success with uniformity has been limited because utilization of the standardized formats created by the various healthcare groups is voluntary. HFMA believes that total uniformity of healthcare administrative processes and systems can only be accomplished if it is mandatory. Federal law must be changed to require all providers and third-party payers to adopt uniform, standard, electronic processes. Without such a requirement, the administrative process will remain complex and cost inefficient.

HFMA's analysis of the administrative burdens currently placed on the healthcare industry can best be summarized by the following points:

- Standard uniform formats and processes for healthcare claims are readily available, but are not used consistently by all participants of the healthcare delivery system.

- With most systems, any request for additional information that is not included in the original electronic format will result in the submission of paper documents, thereby negating the advantages of an electronic transmission.

- Current development of electronic data interchange (EDI) standards have included data transmission standards, but there is no uniform convention for the use of these standards. Any movement by the industry must *require* uniformity, or the industry will be compelled to maintain costly multiple systems.

HFMA COST STUDY

It is widely held that inefficiencies in the current administrative processes are a major contributor to the high cost of healthcare. To substantiate this theory, the Association contracted with Lewin-VHI, a nationally recognized independent consulting firm, to research the potential cost savings once simplification is realized. The study found:

- 1991 administrative costs totaled approximately $126 billion, or 17 percent of total health expenditures.

- Administrative costs for the year can be broken down into three components: $45 billion spent by hospitals; $43 billion spent by physicians; and $38 billion spent by payers.

- It would cost approximately $800 million per year to implement HFMA's proposed administrative simplification processes.

- *Implementation of HFMA's legislative proposal would save $3.4 to $6.0 billion annually.*

HEALTHCARE REFORM PROPOSALS PENDING IN CONGRESS

HFMA is pleased that administrative simplification is a prominent issue in many healthcare reform proposals pending in Congress, including the President's Health Security Act. We have worked very closely with members of the House and Senate, most notably Representatives Thomas Sawyer and David Hobson and Senators Christopher Bond, Donald Riegle and Conrad Burns, who are the chief sponsors of The Health Care Information Modernization and Security Act of 1993 (H.R. 3137/S. 1494), hereinafter referred to as "The Health Care Modernization Act." We are very pleased

that most of HFMA's principles for healthcare administrative simplification and uniformity are included in this bill. It should also be noted that The Health Equity and Access Reform Today Act of 1993 (S. .1770/H.R. 3704), introduced by Senator John Chafee and Representative William Thomas, incorporates most of the Health Care Modernization Act as the method to achieve administrative simplification in a total healthcare reform package.

The following is an analysis of the Health Security Act, the Health Care Modernization Act and three other healthcare reform proposals, based on HFMA's seven principles for healthcare administrative simplification and uniformity. The other proposals, by name, bill number, and sponsor include: H.R. 200, The Health Care Cost Containment and Reform Act of 1993 introduced by Representative Fortney "Pete" Stark; H.R. 3222/S. 1579, The Managed Competition Act of 1993, introduced by Representative Jim Cooper and Senator John Breaux; and H.R. 1200/S. 491, The American Health Security Act of 1993, introduced by Representative Jim McDermott and Senator Paul Wellstone.

Total Industry Compliance

The Health Security Act does not appear to mandate total compliance. Rather, it appears that certain government departments may be separate from some or all of the provisions. The Administration also attempts to provide for state flexibility. While HFMA strongly supports this overall concept, there is concern that flexibility will negate the benefits of administrative simplification. All providers and third party payers must be required to use the same formats. If states are given the flexibility to change or augment formats, uniformity is thwarted. Preliminary documents outlining the Administration's plan mandate only minimum standards for administrative simplification. This will also thwart uniformity. Minimum standards would allow third party payers to require additional input on their forms. It is this additional input that causes the burden, since each payer may desire something different. This would all result in a setback for uniformity among providers and third-party payers.

The Health Care Modernization Act applies to all payers, but only mandates changes to the Social Security Act. Compliance of Federal programs is specifically outlined, as are dates for compliance. Penalties are also mandated. The bill does not allow for anyone to exceed the maximum data in an approved data set. Since the Chafee plan is a total healthcare reform package, compliance would be mandated for all federal programs as well as third party payers, with specific dates for that compliance and penalties.

Both the Health Security Act and the Health Care Modernization Act mandate annual reports to Congress outlining the healthcare community's progress in achieving simplification and uniformity. This will enable changes to be made quickly so that simplification can continue to move forward expeditiously.

The Stark bill would require industry compliance for most payers, but it is less specific when it comes to providers and sponsors. There also appear to be limited exemptions. Additional, more specific language is needed to tighten the compliance requirements.

Representative Cooper's proposal appears to cover all "accountable health plans, public and private third-party payers, providers of health care, and all other entities involved in the transactions." However, the original goals and timetables are voluntary, and if they are not met, the Health Care Standards Commission established by the plan, then promulgates the rules. HFMA's concern here is that the bill appears to allow states to seek waivers for the requirements; this would severely hamper uniformity.

The McDermott bill basically outlines a single payer model. Each state would operate the program and would appear to be the controller of systems for enrollment and state electronic cards. There does not appear to be any acknowledgement that patients cross state lines for service, which would require interstate transactions. Provisions are missing to enable data, once it is entered through various systems, to be made available in a national system. Uniform "reporting" would be required, but states would decide whether or not billing would be electronic.

Use of an Industry Commission Reporting to Congress

The Health Security Act provides for the creation of two councils that would report to the National Health Board: the National Quality Management Council and the National Privacy and Health Data Advisory Council. Neither of these councils has full industry participation and their role is limited. Of particular concern to HFMA is that there does not appear to be any reference to participation by financial managers in either of the two councils.

The Health Care Modernization Act would establish a parent "Health Care Data Panel," comprised of 12 Federal appointees and chaired by the Secretary of the Department of Health and Human Services (HHS). A separate 15 member Health Informatics Commission, comprised of industry representatives, including healthcare financial managers, would report to the panel.

An industry commission would not be required with the Stark bill; rather, the HHS Secretary would implement the regulations. In some cases, the Secretary would take into account recommendations "of current task forces."

The Cooper bill mandates that two boards, the Health Plan Standards Board and a Benefits, Evaluations and Data Standards Board, make recommendations to the parent Health Care Standards Commission. Each board would include industry representatives, and would call on "working groups" of industry managers and technical experts.

The McDermott proposal calls for most transactions to take place at the state level. Several national councils and advisory groups are discussed, but none are specific to administrative simplification.

Electronic Transactions

The Health Security Act contains several different mandates for the use of EDI. There are some requirements for electronic transfer for "those ... that have the capacity," but there is also discussion of "uniform paper forms." Finally, there is a list of "electronic data interchange requirements for those who are automated."

The Administration's reference to the use of standardized paper forms implies that we would continue to rely on paper, not EDI. The Association strongly urges a mandate for standardized *electronic formats*, so that paperless billing results. This will significantly streamline the current system and result in substantial savings.

The Health Care Modernization Act provides for all-electronic processing and the use of clearinghouses and VANS. It also suggests that existing national standards be used, including X12 EDI. Clearinghouses would be certified. HFMA supports such a move to total EDI.

In the Stark bill, electronic transactions and added telephone key pad transmissions are specified. Non-electronic transactions would also be allowed at an additional fee, and paper uniformity standards would be required. The Cooper plan expressly prohibits states from requiring paper-base documents after 1994. Electronic transactions are assumed but not discussed. The McDermott bill, consistently, leaves it up to the states to require electronic billing.

Core Transactions

The Health Security Act includes language for transactions for eligibility, coordination of benefits (COB), claims, payments, disenrollment, enrollment, and utilization review. Specific comments on core transactions are limited, and are more directed toward monitoring, measuring and planning functions. These core transactions are not those identified by HFMA as core transactions. The Health Care Modernization Act includes language for all core transactions as identified by HFMA.

The Stark plan enumerates "core transactions" as eligibility, COB, and billing/claims, with special requirements on laboratory tests. Also mentioned is data for the uniform hospital clinical data set.

Specific transactions are not included in the Cooper plan. Several functions are mentioned in the bill, including: enrollment, eligibility, COB, and claims. In the

McDermott proposal, billing and enrollment are the only two transactions mentioned, and they would be state governed.

Data Maintenance
The Health Security Act specifies an "electronic data network consisting of regional centers" to be established in two years. This network would collect, compile, and transmit information related to enrollment, eligibility, and COB. Employers would be required to update enrollment information monthly.

The Health Care Modernization Act provides for a "uniform working file system" that would hold quality data. While COB is addressed, it is unclear whether eligibility and COB data would be included.

The Stark plan does not discuss a central data base or working file, but provides considerable detail on electronic card requirements. The Cooper bill does not specifically mention a central or regional working file, but does mention national data and local data files. A uniform electronic data base by the year 2000 is mentioned by McDermott, but no details are included.

Confidentiality, Privacy, and Pre-emption of State and Federal Laws Governing Electronic Data with Uniform Identifiers
Both the Health Security Act and the Health Care Modernization Act meet HFMA's principle that Federal law pre-empts state laws regarding confidentiality, privacy and quill pen laws. Uniform identifiers are also included.

While not as detailed as other reform proposals on privacy and pre-emption, the Stark bill covers the issue and calls for some uniform identifiers. Privacy and confidentiality are covered in very broad language in the Cooper bill. Identifiers would be established for beneficiaries and providers. The McDermott plan establishes patient and provider identifiers and addresses confidentiality, but offers no mention of state pre-emption.

Strategic Timetables
The Health Security Act outlines several time periods conditional on other portions of reform. This may result in too much flexibility and may inhibit total uniformity. As mentioned earlier in this analysis, creating a flexible strategic timetable could be problematic if administrative simplification is left to various councils and perhaps state government.

The Health Care Modernization Act includes some initial timeframes that are very detailed and short, especially considering the voluntary/part-time nature of the panel and the commission, and the extended requirements related to quality. The timetable for

implementation of the Act's quality data requirements is more in keeping with a reliable strategic plan. In both cases, however, the proposed timetables may challenge the healthcare community's current capabilities.

HFMA is concerned about the inclusion of waivers in the Health Care Modernization Act. We recognize, however, that there are fair safeguards to ensure that any waivers do not destroy the uniformity standard.

The Stark plan would legislate or regulate almost every timetable, with none calling for industry input. Implementation dates are quite short and do not appear to take into consideration the current complexities and limits of the healthcare system.

Under the Cooper plan, the Health Care Standards Commission would promulgate requirements for implementation for claims and eligibility information. These requirements would be mandated if voluntary efforts failed, and heavy fines would be levied on groups that did not meet the mandate.

The McDermott bill, again, relates all timetables to the state as the single payer. No other mention is made of specific transactions.

ACTIVITIES OF THE INDUSTRY TO ACHIEVE UNIFORMITY

Over the past 25 years, HFMA participated on the National Uniform Billing Committee (NUBC), working closely with other healthcare representatives and the government. The NUBC established the UB-82, a uniform bill form and accompanying data set, to standardize the submission of hospital-based claims. Although the UB-82, approved by the Office of Management and Budget for use in the Medicare program satisfied the goals of a uniform bill, due to a variety of factors, some payers began requiring additional information that was not contained in the uniform bill.

There were about 50 different versions of the UB-82, representing the variances of each State Uniform Billing Committee. There were also as many as 420 different electronic versions of the UB-82, representing various payer versions of this data set. Hence, the uniform bill has not been used uniformly. It has not served to standardize data, and therefore, has not contributed to administrative cost savings.

The UB-82 has now been replaced by the UB-92. This conversion represents two-and-a-half years of work by the NUBC.

In addition to the UB-92, the HCFA 1500 form also is used generally by providers for ambulatory and physician billing. Initially it was only used for Medicare, but recently others in the healthcare community have broadened its use. Since the Medicare program requires all physicians and clinics to bill using the HCFA 1500, many have found it easier to perform all of their billing on the HCFA 1500 rather than use other forms.

It should be noted that the HCFA 1500 and the UB-92 share approximately 95 percent of the same data elements. However, even with the availability of the HCFA 1500 and the implementation of the UB-92, the use of these forms is, and will continue to be, inconsistent. HCFA and other payers may require supplemental claims forms for certain healthcare services. They may also require multiple forms to collect additional requisite information. State laws do not necessarily prevent this situation since, in many cases, the transactions are either regulated by the Federal government or are required by out-of-state payers or administrators. Additionally, ERISA based self-insurance plans are exempt from any state legislative initiatives that attempt to alleviate a state-specific problem.

A provider's economic health is dependent upon the prompt payment of claims. Therefore, providers will continue to respond to payer demands for additional data in different formats. This increases the provider's administrative costs, and therefore, overall healthcare costs.

RELATIONSHIP OF THE INDUSTRY WITH ANSI AND WEDI

In 1989, representatives of several of the nation's larger insurance companies and banks sought to eliminate the use of checks to pay for healthcare claims. Healthcare payers, including HCFA, and providers, specifically HFMA and the American Hospital Association, were concerned about the problems and limitations previously noted. They joined forces with the insurers and banks to form ANSI's Insurance Subcommittee of the Accredited Standards Committee X12. ANSI directed the X12 to develop standard data transmissions between business partners.

Through the X12 and other subgroups, payers and providers have suggested EDI and electronic funds transmission standards to allow for the electronic transmission of large amounts of data and funds. To date, draft standards have been developed for enrollment, eligibility, claims, claim status, payment and remittance, and first report of injury. Task groups have also undertaken projects addressing issues such as utilization review data, crossover or coordination of benefits billing, and other healthcare related data exchanges.

In late 1991, the HHS Secretary convened a summit with the leaders of several of the nation's health insurance companies. The Workgroup on Electronic Data Interchange (WEDI) was a by-product of this summit. WEDI, which included a small representation of healthcare providers, was directed to evaluate the use of X12 standards in the healthcare industry. After several months of deliberations, a report was presented to HHS in July 1992. That report contained an ambitious timetable to implement, with government assistance, many of the current and proposed X12 standards for all healthcare providers and payers by the fourth quarter of 1996. The report also recommended potential legislation if providers do not meet the implementation schedule.

In late 1993, WEDI released its blueprint for streamlined administration of the U.S. health care system. The report continues to support WEDI's original concepts, but calls for a tighter implementation timetable than what was originally projected. For example, WEDI recommended that the adoption and implementation of approved X12 standards be completed by the fourth quarter of 1994 for all payers with 50,000 or more claims or encounters per year, hospitals, nursing home and group practices with 20 or more physicians, and employers with 100 or more employees. All other payers, providers and employers would be required to adopt the standards by the fourth quarter of 1996. Incentives, such as higher tax credits and accelerated depreciation, should be developed to facilitate timely implementation.

While not minimizing the work of the WEDI group, HFMA believes that the group did not fully represent the healthcare community. Consequently, the report's recommendations do not reflect the essential elements to establish a strategic plan for implementation of a standardized system. Furthermore, the report recommends legislative action only after it is proven that voluntary compliance is not effective. HFMA contends that Congress must enact legislation to mandate compliance now, given past experiences with voluntary efforts and the benefits of accelerating administrative simplification.

CONCLUSION

Mr. Chairman, HFMA recognizes the need for comprehensive healthcare reform. We remain convinced, however, that certain key elements of healthcare reform can be enacted quickly. Administrative simplification is one of those key elements. We therefore urge you and the members of your Subcommittee to enact legislation now to simplify and standardize the healthcare administrative processes and not wait for a complete reform package. The concept and underlying principles we have outlined for you today can be effectively integrated into the current system, yet it will also function within any new system. The time to begin moving toward change is now.

On behalf of HFMA, I appreciate the opportunity to appear before you today and present the organization's views on healthcare administrative costs. With more than 31,500 members engaged in the management of healthcare financial operations, we are available to provide guidance to you as decisions are made aimed at simplifying the system. We look forward to working with you, as well as other members of the Congress, the Clinton Administration and, of course, our partners in the healthcare community. Together we must plan the steps necessary to create a national standard, thereby improving our industry, lowering the administrative burdens of health care, and controlling the unnecessary costs brought about by duplication of efforts and paper processing. Thank you.

ABOUT HFMA

- HFMA is the nation's leading personal membership organization for more than 31,500 financial management professionals involved in the financial management of various types of healthcare institutions, including hospitals and clinics, managed care providers, public accountants, consultants, insurance companies, governmental agencies and other organizations.

- Members' positions include chief executive officer, chief financial officer, controller, patient accounts manager, accountant, and consultant.

- Given the geographic and professional diversity of its members, HFMA is in a unique position to identify the problems associated with the current healthcare claims and patient accounting processes.

P:ISSUES\SIMP\STATEMEN.302

Mr. SAWYER. Thank you very much, Mr. Hern.

Mr. Epstein. Am I pronouncing that correctly?

Mr. EPSTEIN. Yes, sir.

Mr. SAWYER. Thank you.

Mr. EPSTEIN. Mr. Chairman and Congressman Hobson and staff, my name is Mark Epstein, and I am presenting testimony on behalf of the National Association of Health Data Organization.

NAHDO is a nonprofit, national membership organization dedicated to improving health through the collection, dissemination, public availability and use of health data.

We cannot emphasize too strongly the importance of this hearing. This forum brings to the fore a critical, but often overlooked building block of health reform: information.

We appreciate the opportunity to present our views on the information needs to support health reform. NAHDO and its members believe that information provides a strong foundation for health reform, and that a comprehensive, nationwide, integrated, publicly controlled health information infrastructure is needed to better understand the health care system and to help monitor and leverage change in the system where change is warranted.

Investing in database development and the maintenance, applications, analyses, and dissemination of information is a prudent investment and a necessary piece of any health reform proposal.

NAHDO has developed a set of principles to guide the collection and analysis and dissemination of information to support health reform. Today I would like to summarize our principles, and please note that a copy of the entire statement of principles is attached to the testimony.

Principle 1. A nationwide health information infrastructure should provide comprehensive data on health status, health system capacity, use, cost, charges, expenditures, and payments, measures of quality of care, and threats to health. A comprehensive information system is needed to meet multiple uses, including assessing and monitoring over time the health status of individuals and populations, developing and allocating health resources to meet identified needs, supporting physician decision making, evaluating what medical and surgical care is effective, measuring provider satisfaction with their care and providers, and guiding health policy.

Principle 2. A public-private partnership is key to a successful nationwide health information infrastructure. The foundation for this information infrastructure and the capacity to support such a system can be found among the states.

Many state agencies now collect, process, and analyze vital health statistics, Medicaid data, data on the use and cost and quality of hospitals and nursing homes and mental health and substance abuse data. States will play an important role in helping to implement health reform, but they cannot shoulder the entire burden.

Private organizations are logical partners. Private health information organizations increase the value of public domain databases when they develop information technologies and innovative approaches for using data which incorporate or can be applied to statewide databases.

Principle 3. Federal guidance is needed to help ensure the quality, completeness, comparability, timeliness, and accuracy of and accessibility to individual level data. We are concerned with what appears to be a top-down emphasize in planning health information systems and the potential burden placed upon state and local governments and private organizations resulting from federal mandates.

Rather, we encourage collaboration and a willingness to build on the strengths and expertise available in both the public and private sectors. The federal government is in a unique position to provide the leadership needed to ensure that health data are standardized and comparable. The federal government can provide necessary guidance by developing uniform or core data sets, standard definitions of data elements, and standard coding and classification conventions, standard reporting formats, unique identifiers for individuals, providers, health plans, and employers, measures of access and outcomes, and privacy and confidentiality safeguards and standards.

States and private industry will find federal guidance useful in developing or modifying their existing data systems.

Principle 4. Sufficient resources should be invested in database development, analysis, interpretation, and dissemination initiatives, information technology, and efforts to enhance present information systems.

We do not advocate for more data as an end unto itself, but for the information and knowledge which is derived from data. We recognize that current resources allocated to health database development are not sufficient to meet the increasing demand for health data arising from health reform.

However, unwarranted expenditures must be controlled by strengthening and enhancing existing health care information systems, not duplicating them. We need to make an investment in database development and its dissemination. These costs include, but are not limited to, developing new databases, converting existing systems or adopting new systems, software development, providing opportunities for staff development and education and training, and funding programs to attract individuals to the health information field.

Too often dissemination of information is neglected. The ability to change data into useful information and then to provide the information to consumers, policy makers, employers or health providers is essential for health reform.

Principle 5. Health data are a public good and should be publicly controlled and collected as close as possible to the data source and available at the community, state and national levels. Health care markets are local. To better understand these markets, assess provider performance and monitor the health of populations, data should be collected as close as possible to the data source or point of service.

NAHDO believes that the most logical regional center for data collection and coordination is at the state level for larger states and a consortia of states in sparsely populated states.

Public agencies act as agents for the public and use public monies to support data collection, analysis, and dissemination efforts.

Ensuring public access to and encouraging use of these data to improve individual and community health is a valuable and worthwhile return on the public investment.

Principle 6. Individual privacy and data confidentiality should be safeguarded at all times. As we move towards health reform, and as information systems are developed, it will be important to address data access issues, such as who owns the data, who has access to the data and under what circumstances, and who monitors those who grant access to the data.

States address these questions today. They have developed data encryption procedures and data security systems, data release and disclosure policies, and other measures to protect individual privacy while making the data accessible. This expertise should not be overlooked, but used.

We hope you and the committee will consider these principles as you move forward.

In conclusion, we commend you for recognizing the importance of information as a tool to change the health care system. We look forward to working with you and your staff on this important issue.

We believe we are uniquely qualified to help identify information gaps in state-wide health information systems. We represent leaders in health information management and analysis from both the public and private sectors, and their perspectives and expertise will be invaluable in developing a practical health information infrastructure which can provide useful information to providers, policy makers, researchers, payers, and the public.

Thank you.

[The prepared statement of Mr. Epstein follows:]

PREPARED STATEMENT OF MARK H. EPSTEIN, EXECUTIVE DIRECTOR, NATIONAL ASSOCIATION OF HEALTH DATA ORGANIZATIONS

INTRODUCTION

Mr. Chairman, members of the Subcommittee and staff, my name is Mark Epstein. I am presenting testimony on behalf of the National Association of Health Data Organizations (NAHDO). NAHDO is a nonprofit, national, membership organization dedicated to improving health through the collection, dissemination, pubic availability and use of health data.

We can not emphasize too strongly the importance of this hearing. This forum brings to the fore a critical, but often overlooked building block of health reform - information. We appreciate the opportunity to present our views on the data/information needs to support health reform.

NAHDO and its members believe that data/information provide a strong foundation for health reform; and that a comprehensive, nationwide, integrated publicly controlled health information infrastructure is needed to better understand the health care system and to help monitor and leverage change in the system where change is warranted. Investing in data base development and the maintenance, applications, analyses, and dissemination of information is a prudent investment and necessary piece of any health reform proposal.

NAHDO has developed a set of principles to guide the collection, analysis and dissemination of data/information to support health reform. Today, I would like to summarize the six principles. Please note that a copy of NAHDO's Statement of Principles is attached to my written testimony.

PRINCIPLE 1: A nationwide health information infrastructure should provide comprehensive data on health status, health system capacity, use, costs, charges, expenditures and payments, measures of quality of care, and threats to health.

A comprehensive information system is needed to meet multiple uses, including assessing and monitoring the health status of individuals and populations, developing and allocating health personnel, developing programs and services to meet identified needs, supporting physician decision-making, evaluating the use, cost and financial stability of health plans, hospitals, nursing homes and other resources, evaluating what medical and surgical care is effective, measuring patients' satisfaction with their care and providers, and guiding health policy.

PRINCIPLE 2: A public-private partnership is key to a successful nationwide health information infrastructure.

The foundation for this information infrastructure and the capacity to support such a system can be found among the states. Many state agencies now collect, process and analyze public health data sets, vital health statistics, Medicaid data, data on health personnel, data on the use and cost of hospitals and nursing homes, and mental health and substance abuse data.

States will play an important role in helping to implement health reform, but states can not shoulder the entire burden. Private organizations are logical partners. Private health information organizations increase the value of public domain data bases when they develop information technologies and innovative approaches for using data, which incorporate or can be applied to statewide data bases.

PRINCIPLE 3: Federal guidance is needed to help ensure the quality, completeness, comparability, timeliness and accuracy of, and accessibility to individual-level data.

We are concerned with what appears to be a 'top down' emphasis in planning health data/information systems and the potential burden placed on state and local governments and private organizations resulting from Federal mandates. Rather, we encourage collaboration and a willingness to build on the strengths and expertise available in the public and private sectors.

The Federal government is in a unique position to provide the leadership needed to ensure that health data are standardized and comparable. The Federal government can provide necessary guidance by developing:

- uniform or core data sets
- standard definitions of data elements and standard coding and classification conventions
- standard reporting formats/requirements for administrative records
- unique identifiers for individuals, providers, health plans and employers
- measures of access and outcomes
- privacy, confidentiality and security safeguards and standards
- 'best practices' or benchmarks
- national reports with community, state, and regional profiles.

States and private industry will find Federal guidance useful in developing or modifying their existing data systems.

PRINCIPLE 4: Sufficient resources should be invested in data base development, analysis, interpretation and dissemination initiatives, information technology, and in efforts to enhance present information systems.

NAHDO does not advocate for more data as an end unto itself, but for information and knowledge which is derived from data. We recognize that current resources - money, staff, technology and time - allocated to health data base development are not sufficient to meet the increasing demand for health data arising from health reform. However, unwarranted expenditures must be controlled by strengthening and enhancing existing health care information systems, not duplicating them. We need to make an investment in data base development and dissemination. These costs include, but are not limited to, developing new data bases, converting existing systems or adopting new systems, software development, data processing and editing, providing opportunities for staff development, education and training, and funding programs to attract individuals to the health information field.

Too often dissemination of information is neglected. The ability to change data into useful information and then to provide the information to consumers, policy makers, employers or health providers is essential for health reform.

PRINCIPLE 5: Health data are a public good and should be publicly controlled and collected as close as possible to the data source and available at the community, state and national levels.

Health care markets are local. To better understand these markets, assess provider performance patterns, and monitor the health of populations, data should be

collected as close as possible to the data source of point of service. NAHDO believes that the most logical regional center for data collection and coordination is at the state level for larger states, and a consortia of states in sparsely populated states.

Public agencies act as agents for the public and use public monies to support data collection, analysis and dissemination efforts. Ensuring public access to and encouraging use of these data to improve individual and community health is a valuable and worthwhile return on the public investment.

PRINCIPLE 6: Individual privacy and data confidentiality should be safeguarded at all times.

As we move toward health reform and as information systems are developed, it will be important to address data access issues such as: who owns the data, who has access to the data and under what circumstances, and who monitors those who grant access to the data? These questions must be answered by the data sources as well as at the community, state and national levels. And these issues must be confronted with an appreciation of and sensitivity to individual privacy and confidentiality and data security.

States address these questions today. They have develop data encryption procedures and data security systems, data release and disclosure policies, and other measures to protect individual privacy while making the data accessible. This expertise should not be overlooked, but used.

CONCLUSION

Congressman Sawyer and Subcommittee members, we commend you for recognizing the importance of information as a tool to change the health care system.

We look forward to working with you and your staff on this important issue. NAHDO is uniquely qualified to help identify information gaps in statewide health information systems - what data are available, accessible to whom and under what conditions; what problems may be faced in developing new data systems and ways to successfully meet those problems; and how the value of existing data bases may be increased by merging or combining them. We represent leaders in health information management and analysis from both the public and private sectors. And their perspectives and experience will be invaluable in developing a practical health information infrastructure which can provide useful information to health providers, policy makers, researchers, payers, and the public.

Thank you.

Mr. SAWYER. Thank you all.

Let me initially turn to my colleague who, like many of us, has other obligations this morning, and so I want to make sure that he gets his questions in first.

Mr. HOBSON. Thank you, Mr. Chairman. I appreciate that.

I just have one question, and I want to thank you all for your help also.

One of the things that I hear from my colleagues when we talk about this, and that you hear from the public, is a fear about privacy. There is some belief today that the records are totally secure, but I am not sure that they really are.

What we have to do is find a way that that belief comes through in the new system. Do you fear the privacy problems or do you think we can solve that not only from an industry standpoint, but from the public standard?

Ms. FRAWLEY. I think it is an excellent point. AHIMA has been very concerned about this issue, the perception that patients particularly have that their information is more secure in a paper based environment, which is certainly why we have been advocating that we need to go forward and move forward to a computer based environment where the appropriate security protections can be built in.

Certainly I know in the next panel you will have a witness you can talk about the role that information technology can play.

I think it is important that we need to have federal legislation to protect the information and certainly do not see any of this as a barrier to building a national information infrastructure for health care, but I do think we need to do a better job of educating our patients and our consumers about this issue.

We need to have federal legislation so that if there is an abuse, there are appropriate remedies, either civil or criminal penalties that can be applied in the situation, but I think that with, you know, a good system design, with certainly the appropriate federal protection, there should be no reason for any consumer in this country to fear abuse of their health information, and that is a major problem right now in our paper based environment.

As much as we do not like to advertise that, it is a concern.

Mr. HERN. If I could speak from a provider standpoint, I tend to share your views, that as you see medical records go back and forth through the halls, you realize that they are fairly available.

Information that we have now in computers is very secure. It has audit trails associated with it and security aspects that go far beyond the current system, and I believe that information will be even more secure on an electronic basis.

Mr. EPSTEIN. I get concerned sometimes that a firm like Nordstrom's or Woodies who knows more about me and my purchasing practices and the colors I like and so forth than my physician who has insufficient information about me. So that would be one response.

There is privacy and there is not privacy, but I think that there are safeguards. Our experience with states in trying to obtain information on hospitalized patients is that states have their own rules and regulations for data release.

We are working on a project funded by the Agency for Health Care Policy and Research which is governed by federal statute and has its own rules and regulations on data disclosure. Let me tell you there are many procedures already in place to insure patient confidentiality at least with hospital discharge data that protects individual privacy. We have been able to help one state, New York, which has particularly rigorous data release requirements learn about what other states are doing. New York is attempting to relax its data release provisions so that researchers can gain access to the data which are essential for looking at the effectiveness of health care, while at the same time protecting individual confidentiality.

So I would support what the previous speakers have said. I think we need to educate ourselves, and I would look to some state experiences.

Mr. SAWYER. Let me follow up on that. Who owns the medical record? Does the patient own it? Does the physician own it? Does each of the care givers and each of their locations own that element of a record that they participated in? Who ought to oversee the judgment about where it ought to repose and how it ought to be released?

Ms. FRAWLEY. Currently, right now, the health care provider owns the record. Twenty-seven states provide a limited right to a patient to access their medical record, which we find very troubling. Certainly in terms of health care reform, if we expect to have educated consumers who can make wise decisions and if we want to move towards a better emphasis in this country on primary and preventive care, we certainly need to allow patients access to their medical records.

Certainly H.R. 3137 does address that need. In the electronic networks, it becomes a little bit more unclear in terms of issues of ownership, and I think that that is something that the IOM report, which was issued in April of 1991, never really addressed.

I am presently working with a work group through the Computer Based Patient Record Institute to deal with some of those issues and hope to develop some guiding principles on that issue because it is somewhat troubling because in a paper based world, it is very clear. Certainly as we build the national information infrastructure, but I certainly think we need to do a better job of making sure our patients have a right to the information and that the patient can control the access and disclosure of information.

So I think those are some important provisions that we need to address.

Mr. SAWYER. And have the opportunity to correct and amend.

Ms. FRAWLEY. Right. Very important.

Mr. SAWYER. Other comments? Sure, go ahead.

Mr. EPSTEIN. In following up on a point that was just made, I think one question is who owns the record, but there are others such as who has access to the data in the record. We are concerned about, and we do not necessarily have an answer, to who determines who has access to those data and for what purposes. Who is watching those who determine who determine who have access to the record?

Mr. SAWYER. We are talking about an enormously fragmented system that will come together piece by piece if we set the standards well. I was asked a question yesterday that I think is probably best answered the way Dave expressed it in his testimony, that this system does not cost money; it saves money, but somehow that is often not a sufficient answer for those who are thinking in those terms.

How do we begin to quantify the costs and benefits of such a system, and how do we ascribe those costs across everything from the personal computer on the desk of a physician's office to the large repositories that will have to be a part of such a system?

Mr. EPSTEIN. I do not have a number. They may have a number, but I am suspicious of those who have numbers.

Mr. SAWYER. Yes, but I am asking how do we begin to really measure this sort of thing.

Mr. EPSTEIN. I think you have to look, in part, at what is already in place, and we (NAHDO) receive calls, for example, from existing states that want to set up data systems, be they hospital discharge data or other data systems, and they want to know how much does it cost; how long will it take; typical questions.

And we will say, you can call California. You can call Ohio, et cetera, and ask them what it takes.

The cost estimates are grossly underestimated, I suspect, because they do not include other factors such as trained staff, rules and regulations, and all of the process that has to be gone through to develop the infrastructure.

And there is the people and their training that may or may not be avaliable. In a public setting, it is difficult to sustain people at least at the state level because of the uncertainty of funding, or the lack of sufficient funding.

The element that is often lacking, and it is unfortunate and so we emphasize it, is the dissemination role. Too often the information is collected. It is put into a report, and the report is not understandable by anyone except the person who may have provided the report, perhaps not even those which have provided the information.

I think dissemination is usually underfunded, and underappreciated because nobody is going to, I suspect, support data in and of itself unless it can be translated into that information that is understandable. I think that within the field itself, we are woefully lacking in our ability to disseminate.

All you have to do is attend a professional meeting like one that we put on and look at the presenters. We cannot communicate to ourselves, let alone to policy makers or to providers. So those are some of the factors that I would put into the equation as you start the calculation, and then add on ten percent or whatever.

Mr. SAWYER. Mr. Hern.

Mr. HERN. We do know that business functions are costing providers somewhere in the vicinity of $125 billion a year, and from the study that I referenced before, we can save at least three to $6 billion of that, but the issue of how do you get your arms around the cost of the medical record data and those processes is extremely difficult and, again, talking from my role on the provider's side, and we have looked at that, our organization is moving toward

electronic medical records and those kinds of technologies. We really could not measure it. All we knew was that from a strategic standpoint, that there was significant savings associated with it when done properly.

It comes from gains in productivity and improved health care outcomes to patients, and it is immeasurable, but we do know that we will save substantial amounts of dollars.

Mr. SAWYER. Time is money. How long is this going to take? We have got some time tables that are nominally built into the legislation as drafted, but I do not think any of us have any enormous confidence in where those time tables lie and what the task is that is before us.

Clearly, it is going to require some flexibility, but can you illuminate for us at all how long you think it ought to take us to put such a system in place?

The fact is many of the things that we hope for in terms of cost containment over time, the avoidance of the brick wall that we were talking about in terms of reversing whatever gains have been made in terms of deficit reduction, really will depend on some of the gains that we would make and measured in these terms.

How far down the road are we?

Ms. FRAWLEY. Well, I think that in terms of computer based patient records, we are still several years away and primarily because of the fact that the standards that we need to bring that technology forward have not been developed.

I think an important first step certainly is administrative simplification, and I think certainly all of us here this morning can agree on that point. There certainly has been a number of reports, most notably the reports issued by the Work Group for Electronic Data Interchange, that laid a foundation that we certainly could very quickly implement within the next year.

Certainly if we can start, you know, electronic data interchange for claims processing, starting to standardize data sets, starting to standardize our claims forms, we can begin to build that electronic highway, and certainly if we can accelerate standards development and move more quickly towards computer based patient records.

The major stumbling block there, of course, is going to be the cost, and certainly none of us here can even quantify, you know, what that potential cost is, but I think for providers if we can begin to streamline the billing processes, if we can begin to streamline all of the duplicative data collection that is now ongoing, that the providers are currently experiencing, and to begin to build that electronic highway, then certainly that becomes a greater reality.

Mr. HERN. I think we believe it will take a minimum of three to five years, and you said time is money. Well, money is time, and I think that three to five years could accelerate or could slow depending on how quickly the cost of technology drops. Some of these aspects are extremely expensive right now, and the cost benefits are not there immediately, but will be there in the near future.

Mr. EPSTEIN. I do not know, but I know that there is a good bit of experience both in the public and private sector to learn from, and we have heard some of this.

I would go back and say at the state level and at the national level, there are a number of efforts underway. These experiences

should be gleaned or tapped to see what some of the potential obstacles are, and I do not say that lightly.

We are dealing not only with technology, but we are dealing with people and peculiarities in rules and regulations, and the processes may be slower than the technology.

One final example. The State of Kentucky passed last spring a bill to set up a health data commission. It had a very broad mandate, and was well funded, and it had five commissioners none of whom had much background in health information systems. We were invited to Kentucky to help them and give them a perspective on what is happening around the country.

One of the commissioners finally said how long will it take before we can issue our first report using hospital discharge data. This is a relatively easy system to develop. There may be 100 to 130 hospitals in the State of Kentucky.

I said you mean from today when you have no staff. You have no rules, no regulations, no equipment, no data definitions, no reporting form, no idea of what this report is going to look like. A minimum or ball park figure of maybe two years, I said.

That is unacceptable, the Commissioner said, that is reality, I think reality will affect this, but I think there is experience upon which to tap and to help move it along a bit faster.

Mr. SAWYER. Well, thank you all very much. I hope that you will be prepared to answer whatever subsequent questions that we may have in writing. I am enormously grateful for the quality of your presentations this morning. You have helped us get off to a good start, and we look forward to our work with you as we proceed.

Thank you very much.

Ms. FRAWLEY. Thank you very much.

Mr. HERN. Thank you.

Mr. EPSTEIN. Thank you.

Mr. SAWYER. Our third panel this morning will consist of John D. Lacopo, who is Vice President of Governmental Affairs for EDS, and John Rahiya, Vice President for Health Care Information Systems of Equifax.

Gentlemen, it is a pleasure to have you here this morning.

Mr. TISDALE. Actually for EDS this morning, Mr. Chairman, it will be myself, Pat Tisdale. I am the Vice President of EDS' Health Care Division.

Mr. SAWYER. Thank you for your correction. I appreciate it.

Why don't we proceed in the institutional order in which you were introduced then?

Let me emphasize again just for the record that the full text of your statements will be made a part of the record, and you should feel free to emphasize and focus in any way you want.

Thank you.

STATEMENT OF PAT TISDALE, VICE PRESIDENT, HEALTH CARE, EDS, AND JOHN RAHIYA, VICE PRESIDENT FOR HEALTH CARE INFORMATION SYSTEMS, EQUIFAX

Mr. TISDALE. Thank you.

Mr. Chairman and members of the subcommittee, again, I am Pat Tisdale, Vice President of EDS' Health Care Division.

I am pleased to be here this morning to discuss our nation's health care information infrastructure. Before I begin, I want to congratulate you, Mr. Chairman, for the leadership you are bringing to this important issue and for the efforts of Congressman Hobson, and Senators Bond and Reigle.

I believe that your legislation will, in fact, help facilitate the expansion of our health information network.

There are two main points that I would like to make in my testimony today. First, efforts to solve some of our nation's most difficult health care problems have been hampered by the absence of timely and complete data on the health care experience of our population.

Second, our ability to generate and share these data depends on continued investment in health care information systems, particularly electronic medical records and a coherent communications infrastructure.

Currently any research that requires information from patient charts relies on medical records abstracting. This is a time consuming, expensive, and often imprecise data collection technique. Computerized patient information can be retrieved, aggregated, and analyzed faster, cheaper, and more accurately. This will enable better health research, including medical outcomes studies and randomized clinical trials. Research that used to take years will now, in fact, take months.

Electronic patient records are already beginning to improve patient care within individual health systems. For the full potential of electronic medical records and other health information systems to be reached on a national basis, however, they must be supported by a cost effective telecommunications infrastructure.

The current telecommunications infrastructure is of sufficient quality to enable electronic data interchange, an example being for claims submission and payment. With respect to health care delivery, however, many applications are already stretching the capabilities of the infrastructure. Teleradiography, for example, requires high speed telecommunication networks to transmit diagnostic X-rays and other images from one location to another. Due to inadequacies in our current infrastructure, there are relatively few places in the United States where teleradiography is being used.

Future infrastructure applications, such as visual representation and natural language recognition, will require integration of telecommunications technologies to include fiber, wire, satellite and cellular. High speed, on-demand communications networks will be the rule.

Mr. Chairman, some critics of computerized health care data contend that personal privacy will be sacrificed as the price we pay for a manageable health care system. For some reason, as we talked earlier here, the chart cart, file room, and the U.S. mail are thought to be more secure than computer networks.

Today many people, most of whom have no responsibility or relationship to the patient, have access to the information in the paper based medical record. Technology's greatest contribution to protection of privacy is in its ability to create strong, effective security systems.

These systems can control and record who has access to what data and under what conditions. They also allow us to process and move data electronically and anonymously. Use of security devices and procedures, such as encryption, passwords, and biometrics, such as fingerprints and retinal scans, can significantly reduce unauthorized access to medical information. The sophisticated audit trails will allow investigation of who, when, and how particular information has been accessed.

In the computerized environment, research can be done with sanitized data. Analytical programs can strip away name, address, and other identifying characteristics from records prior to analysis.

With respect to public policy, EDS supports limited government intervention to achieve uniform data standards, preemptive privacy legislation, and telecommunications infrastructure enhancements. Of all the legislation that has been drafted to achieve data standardization and administrative simplification, EDS feels most comfortable with the approach set forth in the Hobson-Sawyer bill.

This legislation will create an explicit, public-private partnership in all aspects of our national health information infrastructure. Under H.R. 3137 the primary role of the federal government would be to eliminate barriers to the creation of infrastructure and to assure compliance through the establishment of realistic enforcement mechanisms.

All federal and state programs would be required to use the same standards as the private sector, insuring interoperable networks and consistency of data.

The private sector will be encouraged to build upon existing infrastructure, helping to minimize expensive and unnecessary redundancy, as well as the issue of time.

The legislation is technology neutral as proposed, allowing maximum flexibility to incorporate new technologies as they are developed.

The most important contribution that can be made in terms of privacy by the Congress is to establish a national policy. Without rationalizing the current patchwork of state laws, it will be virtually impossible to create the protections and the efficiencies possible through computerization of our health care information, especially on an interstate basis.

In the absence of policy guidelines, systems will be built now that may not meet future requirements and will necessitate extensive, costly retrofitting.

Finally, the federal government should take steps to facilitate the implementation of an enhanced telecommunications infrastructure. At a minimum, the government should support tax incentives to stimulate investment in the infrastructure and should act to promote local exchange competition, essentially the gateways to these networks.

In addition, government should provide a legal and regulatory environment that is conducive to network modernization and create predictable, but adaptable laws and regulations for the communications industry.

In conclusion, Mr. Chairman, EDS stands ready to work with you and your committee and the administration in passing appropriate

administrative simplification, privacy and telecommunications legislation during the 103rd Congress.

Thank you for your efforts and please do not let up.

[The prepared statement of Mr. Tisdale follows:]

PREPARED STATEMENT OF PAT TISDALE, VICE PRESIDENT, HEALTH CARE, EDS

Mr. Chairman and members of the Subcommittee, I am Pat Tisdale, Vice President of the Health Care Division of EDS. I am pleased to be here this morning to discuss our nation's health care information infrastructure and how it can be leveraged to help solve some of our nation's pressing health care problems.

Before I begin, I want to congratulate you, Mr. Chairman, for the leadership you are taking on this critically important subject. The Health Information Modernization and Security Act (H.R.3137/S.1494) introduced by you and Mr. Hobson in the House, and by Senators Bond and Riegle in the Senate, would make great strides in facilitating the expansion of our national health information infrastructure.

Based just outside Dallas, Texas, EDS is a major provider of information technology (IT) services including consulting; systems development, integration, and maintenance; and process management. EDS' 1993 revenues exceeded $8 billion and our leading markets include federal, state and local government; health care; insurance; communications; manufacturing; transportation; financial services; energy; and retail services. We employ more than 71,000 people in 31 countries.

EDS has been providing IT services to the health care industry for more than 30 years. Our health care customers in the private sector include Blue Cross and Blue Shield plans, commercial insurance companies, providers, and managed care organizations. As the provider of claims, membership and client reporting services for NASCO, the National Account Service Company for various Blue Cross and Blue Shield plans, EDS supports 66 of their plans in areas covering 90 percent of the population. In addition, EDS supports the administration of the health plans of our parent company, General Motors. With respect to the federally financed programs, EDS is the largest processor of Medicaid claims nationwide, and we provide Medicare Part B information processing services in 10 states.

Mr. Chairman, there are three main points I would like to make in my testimony today. First, efforts to solve some of our nation's most difficult health care problems have been retarded by the absence of accurate, timely and comparable data on the health care experience of our population. Second, our ability to generate and share these data hinges on continued investment in health care information systems, particularly electronic medical records, and a coherent communications infrastructure, such as the National Information Infrastructure proposed by Vice President Gore. Regardless of what other health reforms may be enacted by Congress this year, action should be taken to facilitate rapid deployment of our health care information infrastructure. Third, strong federal privacy protections are imperative to ensure the integrity of the infrastructure. Without these protections, the public may rebel against further automation of their personal medical data and the private sector will continue to be hampered in the development of interstate health information networks.

THE VALUE OF ELECTRONIC HEALTH DATA

Many of us in the health care field -- practitioners and policy makers alike -- share a vision of the 21st century health care system. It is a system where all Americans are able to access medically necessary and appropriate health care services, regardless of their geographic location or income level. It is a system that emphasizes health rather than sickness and rewards the individual for adopting and maintaining a healthy lifestyle. It is a system that supports good decision making by patients and providers through easy and immediate access to the comprehensive information required to make sound health care-related decisions. And it is a system with far less administrative waste, hassle and paperwork.

Ironically, health care is one of our most information intensive industries, yet it is one in which IT has been taken advantage of the least. Each patient encounter with the health

care system -- and there are well over a billion each year -- generates massive volumes of data: medical, financial and administrative. Unfortunately, most of this data has been captured and stored on paper -- in hundreds of different formats -- making it difficult to retrieve, aggregate and analyze. As a result, our ability to generate useful information to support coverage and care seeking decisions of patients and treatment decisions of providers has been sharply curtailed.

Fortunately, all that is changing. Faced with growing competitive and financial pressures, health care delivery systems and insurers are re-engineering their business practices and re-tooling their workforces. Information technology and connectivity have become important components of many of these restructurings.

While the first wave of health industry connectivity has been focused on streamlining claims submission and payment, increasingly these networks will be used to share clinical information for direct patient care and research purposes. The tool that offers the greatest promise for reaching this vision is the electronic medical record (EMR).

As a division vice president of a company that has pioneered EMR technology over the past several years, I can tell you that this technology is, relatively speaking, in its infancy. There are other forms of personal health data that are far more automated at this point in time, most notably health insurance claims data and clinical encounter data from managed care organizations. Nonetheless, EMR-related technology is being applied in varying degrees in many health care organizations, and we are clearly moving toward a time when paper-based medical records go the way of housecalls and the doctor's black bag.

What constitutes an EMR varies by organization, but in general all information pertaining to patient care--clinical, administrative and financial--is entered directly into a computer at the time services are rendered. In marked contrast to the current

environment, in which the patient chart is unavailable about one out of every three times care is given, EMRs assure provider access to complete, legible information all the time. Orders for tests, procedures or prescriptions are entered on-line and automatically forwarded to the appropriate location (lab, pharmacy, etc.) for action. Test results, which are now lost in more than 10 percent of cases, are entered directly into the system, often with prompts to the provider regarding patient follow-up.

In addition to the obvious cost and quality benefits at the individual patient level from having provider access to complete, legible information at all times, EMRs offer significant societal benefits as well. Currently, any research that requires information from patient charts relies on medical records abstracting, a time consuming, expensive and often imprecise data collection technique. Through the use of database technologies and electronic data interchange, computerized patient information can be retrieved, aggregated and analyzed faster, cheaper and more accurately. This will enable more and better health services research, such as medical outcomes studies, as well as expanded quality improvement initiatives.

Biomedical research and randomized clinical trials, of new prescription drugs for example, will also be facilitated by EMRs. Research that used to take years, if not decades, will be done in a matter of months, with faster and more direct dissemination of important findings to doctors and other clinicians.

Electronic patient records are already beginning to improve patient care within individual health care delivery systems, such as the Harvard Community Health Plan. For the full potential of EMRs and other health information systems to be reached on a nationwide basis, however, they must be supported by a comprehensive, seamless, cost-effective telecommunications infrastructure.

78-232 O - 94 - 3

HEALTH DATA AND THE NATIONAL INFORMATION INFRASTRUCTURE

Supporting our current health care system is a conglomeration of both "hard" and "soft" technology, operating within a larger legal and regulatory environment. The "hard" technology is often identified as the infrastructure because it is the tangible, easy to see and touch portion of the system which includes wires, transmitters, receivers, computers, switches, peripherals and terminals. However, it is the "soft" technology which turns data into information, and which creates meaning and value for an organization or a society. The soft infrastructure includes common data formats and protocols, processes for navigating and querying databases and networks, and programming methodologies which allow easy assembly of data into useful information.

This subtle twining of network, computer, software and services technology together with the laws, regulations and policies which shape how it is deployed, creates our National Information Infrastructure (NII). Improvements in the hard and soft infrastructure, technological and legal, are required in order to positively impact the health care community's ability to apply information technology.

The current telecommunications infrastructure provides acceptable connectivity and quality to enable providers and insurers to electronically exchange financial and administrative data. That is, the infrastructure supports medium speed private line data transmission of sufficient quality and reliability to facilitate electronic data interchange (EDI) for claims adjudication and payment purposes. Throughout the country EDI linkages are being established between payers and providers to eliminate the paperwork and reduce the costs associated with health benefit plan administrative functions: enrollment, eligibility verification, claims submission, remittance advice, and payment.

With respect to health care delivery, however, many IT applications are significantly stretching the capabilities of the existing telecommunications infrastructure. In fact, transmission of large amounts of clinical medical record data would require a private network on top of the public network to obtain features that the public infrastructure cannot provide. Examples are applications which require large amounts of computer data to be transmitted on demand at very high speeds. Local area networks provide such capability in campus environments. In today's health care industry, however, resources are frequently geographically dispersed. The communications infrastructure must supply the necessary connections to these resources.

Teleradiography, for example, requires high speed communication networks to transmit diagnostic x-rays, magnetic resonance images, computerized tomography scans, positron emission tomography scans, sonograms, echocardiograms, and thermograms from one location to another for immediate consultation. Due to inadequacies in our current infrastructure, there are relatively few places in the United States where teleradiography is being used. This is unfortunate, since teleradiography and other telemedicine applications offer enormous promise for improving access, quality and satisfaction with health care delivery in rural America.

Future requirements of our health care information infrastructure will likely include visual representation and natural language recognition. For this to happen substantial infrastructure enhancements are necessary. Not only will health care providers need reliable high-speed networks of data transmission quality between themselves, but the infrastructure may also need to carry similar communications to individual households. Integration of all telecommunications technologies including wire, fiber optics, satellite, and cellular becomes a prerequisite. High speed communication (at variable speed) on demand will become the rule. Such infrastructure enhancements may require sizable

capital investments, particularly at the local exchange level that connects the households.

Health Information And The NII Demand Security & Confidentiality

The movement toward the EMR and a ubiquitous communication system has clearly made the issue of privacy and confidentiality of personal health data more visible, although no more important, than it has ever been before. Some critics of computerized health care data contend that personal privacy will be sacrificed as the price we pay for a manageable health care system. They believe that there is an implicit and absolute trade-off between greater availability of individually-identifiable information and risk of personal privacy and confidentiality violations.

In contrast, I would suggest to this subcommittee that through the application of IT within the context of an explicit data security policy, as I will describe, we have the potential to both increase the availability of information and reduce the overall risk of privacy violations that we encounter in today's paper-based health care system. Just as technology is a tool to enable more effective information collection and use, it is also the tool to enable greater security of the data itself.

Computerized Systems Provide Greater Protection Than Manual Systems

The perception that computerized systems are somehow more vulnerable to invasion than manual systems is inaccurate. For some reason, the "chart cart," file room, and U.S. mail are thought to be more secure than the computer network. In reality, today's system of moving patient files from place to place requires that many people, most of whom have no responsibility or relationship to the patient, have access to the information in the patient's medical record.

Technology's greatest contribution to the protection of privacy is in its ability to create strong and effective security systems. These systems not only control and record who has access to what information under what circumstances, they perform many of the administrative tasks of processing and moving the information electronically and anonymously.

Here are some of the ways in which technology can contribute to increased confidentiality protections:

1. Security Techniques and Audit Trails. Use of security devices and procedures such as data encryption, passwords, badges with personal identification numbers (PINs), biometrics such as fingerprint and retinal scans, and many others can significantly reduce the number of violations due to casual, accidental or amateur intrusions. Automated systems also enable sophisticated audit trails. Such auditability can allow investigation of who, when and how particular information was accessed.

2. "Sanitization" Technique. Computerization provides unparalleled opportunities to make massive amounts of medical information available – quickly and anonymously -- for research purposes. This research is critical for understanding outbreaks of diseases, as well as for determining optimal treatment and cure ratios. In a computerized environment, this outcomes analysis can be done with "sanitized" data, by having the analytical program "strip" away specified pieces of data from the records during the aggregation process. In this way, name, address, and other identifying characteristics can be removed prior to data analysis.

One may look at the possibilities for studying computerized data and be fearful of "big brother" accessing anyone's file at any time for any purpose. But a realistic assessment of this situation can only be made in light of how research is conducted in today's paper-based environment. Literal armies of researchers are authorized to cull through

thousands of individual patient charts. The abstractors must often search the entire chart (sometimes hundreds of pages in length) for just a few pieces of information. As a result, these people often see much more information than is relevant to their particular study. Not only is this system costly and inefficient in producing the type of data necessary, it relies solely on each individual researcher's ethical behavior whether additional personal information is disclosed. In an automated system, many of the disclosure decisions are removed from the researcher, since he or she is never allowed access to non-relevant information.

3. Networked -- Rather than Centralized -- Information. Opponents of EMRs and other forms of electronic health data suggest that because computerization can "centralize" records, they are more vulnerable to inappropriate access. These critics often assume that the "centralized" data will reside in one place and that only one set of locks must be picked to gain access to everyone's information. In fact, when computerized data is "centralized," this does not mean that it resides in a single physical location. Health care data reside in thousands of computers around the nation, and once EMRs are universally implemented, data will reside in hundreds of thousands of computers. EDS is involved in a number of groundbreaking attempts to build statewide EDI networks that will allow providers, payers and government agencies to share patient information (clinical, as well as administrative) without the data residing in a single, centralized database.

TECHNOLOGY ALONE IS NOT ENOUGH

The responsible implementation of IT to help protect patient information is one of the strongest links in the confidentiality chain. The weakest link is often the work processes and procedures that the technology supports. IT can most effectively be developed to secure a system if a strong confidentiality and security policy is in place, including a

clear definition of "authorized access" for each type of information protected and training and education for individuals authorized to use the system.

Security procedures can be built into the system to protect different types of information to different degrees, but these categories must be defined, along with criteria for accessing them. Training is essential to ensure the users comprehend the purposes of the security systems, how to operate them, and what penalties will be imposed if they abuse their privileges and access information for inappropriate purposes.

PUBLIC POLICY RECOMMENDATIONS

EDS supports limited government intervention to facilitate the development of a nationwide health care information infrastructure. It is our belief that a few key actions by the federal government will speed the development of a technological infrastructure that can be applied to generate the information needed to bring about marked improvements in the quality and cost-effectiveness of health care delivered in this country. Specifically, Congressional action should be directed toward system wide adoption of uniform data standards; preemptive privacy legislation; and telecommunication infrastructure enhancements.

Of all the legislation that has been drafted to achieve data standardization and "administrative simplification", EDS feels most comfortable with the approach set forth in your legislation, Mr. Chairman. The Health Information Modernization and Security Act would assure an explicit public-private partnership in all aspects of our national health information infrastructure.

Under H.R.3137, the primary role of the federal government would be to eliminate barriers to the creation of the infrastructure and to assure compliance through the

establishment and implementation of a realistic monitoring and enforcement mechanism. All federal and state health programs would be required to use the same standards as the private sector, thereby ensuring interoperable networks and consistency of data. The private sector would be encouraged to build upon existing infrastructure, helping to minimize expensive and unnecessary redundancy. Of tremendous importance, the legislation is technology neutral, allowing maximum flexibility to incorporate enhancements and new technologies as they are developed.

With respect to health data privacy, while there will be large pressures on Congress to micro-manage the implementation of technology to ensure patient confidentiality, Congress should resist that temptation. There are many technological paths to ensuring a secure and private system. In fact, overly specific mandates on the technologies or technical processes to be used can undermine confidentiality and security by giving invaders important clues as to the type of locks they can try to pick.

The most important contribution Congress can make in the privacy arena is to establish a national policy outlining the objectives, measurements and accountability for the use and protection of patient information. Today's system of inconsistent state laws makes it difficult, if not impossible, to use computerized systems across state boundaries. This is a particular stumbling block to the development of health care networks bringing clinicians, hospitals, insurance companies and researchers together to better manage the delivery systems operating in their communities. Without rationalizing the current patchwork of state laws governing the privacy of medical data, it will be impossible to achieve the protections and efficiencies possible through computerization of our health care system.

EDS has joined the Workgroup on Electronic Data Interchange, the Institute of Medicine, the American Medical Association, the American Hospital Association, the

American Civil Liberties Union, and the American Health Information Management Association in calling for preemptive privacy legislation. With appropriate Congressional guidance on key policy issues, such as what constitutes invasion of privacy; what types of information should be protected and to what degree; what constitutes authorized access/use; and penalties for violations, it will be possible to take advantage of technology to meet these requirements in a cost-effective manner. In the absence of this policy guidance, systems will be built now that may not meet future requirements. The cost of retrofitting these systems with privacy features could be prohibitive.

Last, but definitely not least, the federal government should take steps to facilitate the development and deployment of an enhanced telecommunications infrastructure. At a minimum, government should implement tax incentives to further stimulate investment in the infrastructure and should act to promote local exchange competition. The bulk of infrastructure investment needs to be made in the local loop, but today it is controlled by entities that are not forced by competition to make the right decisions. In addition, government should provide a legal and regulatory environment that is conducive to network modernization by creating predictable, but adaptable laws and regulations for the communications industry. As part of this process, government needs to assess the tradeoffs between universal service, rate equity, and related levels of service.

Historically, the primary purpose of telecommunications policy has been to ensure widespread availability and affordability of phone and video services. These traditional objectives remain. In parallel, observers recognize the need for more advanced services required to contribute to business success. This creates an increasing number of conflicts between more diverse goals. Achieving overall consensus becomes more difficult. Simply put, we need an approach that balances the multitude of interests while recognizing that no single segment of society can shoulder the entire burden. At

the same time, government can and should aggressively pursue a policy of assuring easy and open interconnection to public networks.

In conclusion, Mr. Chairman, EDS stands ready to work with you, your Congressional colleagues, and the Administration in passing appropriate administrative simplification, privacy, and telecommunications legislation during the 103rd Congress. We applaud your efforts to date in this regard and urge you not to let up, so we can pass these items this year and hasten the building of the national infrastructure necessary to support a more efficient, effective health care system.

Mr. SAWYER. Thank you, Mr. Tisdale.

Mr. Rahiya.

Mr. RAHIYA. Good morning. Mr. Chairman and members of the subcommittee, I am John Rahiya, Vice President of Equifax, Inc., and I am pleased to testify today on behalf of Equifax on the critical issue of information systems characteristics and information policy principles that will be needed to support health care reform.

In the interest of time, I will summarize my more detailed written statement, which I ask be included in the record.

Mr. SAWYER. Without objection.

Mr. RAHIYA. Thank you.

It will be impossible for any health care reform 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.

Mr. Chairman, you and the members and staff of this subcommittee are to be commended for recognizing the importance of effective and responsible management of health information in health care reform. Equifax is looking forward to working with you on this critical issue.

Equifax is the leading provider of discrete personal information and services to support consumer financial transactions. Our 94-year history has focused on that effort. We manage large databases with millions of on-line data sets. We update our databases over a billion times a month, while serving 60,000 demanding customers over two million times a day.

Equifax does so with sophisticated information technology, and we do so with a passion for protecting the personal privacy of individuals upon whom we manage, store, and release information.

Mr. Chairman, let me reemphasize those characteristics of our company because they relate so directly to the challenge of designing and developing a health information infrastructure.

Our history is one of dealing with highly sensitive individual information, leveraging it with state-of-the-art technology, and surrounding it with a passion for personal privacy protection. It is really why we are able to exist every day.

In our health record businesses, Equifax has handled health record data for many decades and always with special care. Equifax follows company-wide fair information practices which surpass current legal requirements in the privacy area.

Health care reform initiatives call for provider performance and quality measurement, and less costly administration—I almost said more costly—administration, I do not think that is what we are after. Their success will depend and result from automation and greater aggregation of personal health information. Medical outcomes analysis, research and health care management can then be better addressed.

Simply stated, personal health information will and is becoming more accessible for more uses. Privacy concerns demand that proper safeguards be established and strictly followed. Our experience can validate that last point.

The existing health record information infrastructure is a somewhat disjointed patchwork of databases and systems with information generated and held at a variety of points. The handling of

health records is heavily regulated, but not in a comprehensive or consistent manner.

We applaud the effort of H.R. 3137 to emphasize the need for integration and uniformity.

A new health care information infrastructure is emerging. The developing automated patient record will be used for medical, payment, research, and quality measurement decisions and will by its nature include sensitive personal information.

In reforming the health care system, this Congress has an opportunity to guide the restructuring of health information systems in a way that maximizes the utility of the health record while protecting personal privacy.

If Equifax can contribute to your efforts, and we want to do so, it will be by sharing with you in the few minutes I have remaining some of our experiences in applying technology to sensitive personal information where privacy protection is critical.

The statements, what use, what data, and what source, are the threshold questions in any effort to structure a responsive information system. When you are in the information business, as we are, these questions are repeated daily. They are the acid test for the data component piece of an information system.

Information systems must be user driven. The key to a workable system is to identify legitimate users, understand their information needs, design the system to meet those needs. Such systems may feature large heterogeneous databases and open architecture to serve numerous and varied users.

The data sources for health information systems will vary greatly. Thus, the systems must be designed to safeguard the integrity of the personal data.

With respect to unique identifiers, there is a difficult and ongoing challenge in matching the right data with the right person. This is a single point of failure in any information system.

The President's task force makes a reasonable point, in our view, in recommending a unique national identifier.

Regarding decentralization and uniformity, it would be expensive, inappropriate, and counterproductive to supplant existing databases with a centralized database. H.R. 3137 takes the correct approach in assuming that there will be numerous and different information systems that will comprise the health information infrastructure and in mandating standards for the interchange of information among these systems. This is essential.

Regarding security, a decentralized database architecture places a premium on security. A key component of security is access. This is a subject to which Equifax has given enormous attention and devoted significant resources in both our consumer and our medical information systems.

A national health information system will require mandatory state-of-the-art security standards, such as procedures for audit trails and data encryption. I cannot overemphasize the importance of data security, particularly who has access to what information.

On the point of privacy, Equifax has taken the lead in creating stringent privacy procedures for the handling of personal medical information. This is in keeping with concerns Americans have ex-

pressed about the privacy of their health information outside the direct care-giver community.

In 1993, we sponsored a nationwide health information privacy survey conducted by Louis Harris & Associates. The survey found that 83 percent of the public and 93 percent of health and government leaders believe that it is important that organizations handling and reviewing personal medical records should have detailed privacy and confidentiality policies.

We have an internal task force and outside experts working to apply the company's existing fair information practices to the expanding application of information technology in the health care field. Heath information privacy principles and fair information practices must include standards for the collection of information, uses and access of data, accuracy of information, disclosure of information, and participation rights by the data subject.

Interestingly, our 1993 survey found that 61 percent of Americans have concerns that their medical information is being seen by many organizations beyond those that need to see them for health care services. Further, the survey found that 56 percent of the public and 57 percent of health and government leaders favor enacting comprehensive federal legislation that spells out rules for confidentiality of individual medical records.

Equifax shares this public sentiment and looks forward to working towards legislation that appropriately balances safeguards, access, and uses of individual health information.

In conclusion, Mr. Chairman, Equifax believes that effective information systems and information policies are imperative for successful health care reform. While the technology exists for interconnecting systems and exchanging information, protecting data and personal privacy remain to be fully developed. I can assure you this process will take time.

Equifax welcomes the opportunity to share its expertise with the Congress and the administration on both the technical and privacy aspects of developing health information systems. We look forward to continuing to work with Congress.

We thank you for this opportunity to testify.

[The prepared statement of Mr. Rahiya follows:]

PREPARED STATEMENT OF JOHN RAHIYA, VICE PRESIDENT FOR HEALTH CARE INFORMATION SYSTEMS, EQUIFAX

INTRODUCTION

Mr. Chairman and Members of the Subcommittee, I am John C. Rahiya, Vice President of Equifax, Inc. I am pleased to testify today on behalf of Equifax on the critical issue of the information system characteristics and information policy principles which will be needed to support health care reform.

Most of the congressional and public focus on health care reform to date has, of necessity, been on threshold issues such as financing, coverage and quality of care. However, it will be impossible for any health care reform plan to succeed unless there is also in place an effective, efficient and privacy sensitive information infrastructure to collect, maintain and transmit essential personally identifiable health record data.

Mr. Chairman, you and the members and staff of this Subcommittee are to be commended for recognizing the importance of effective and responsible management of health care information in health care reform. Equifax is looking forward to working with you on this critical issue.

EQUIFAX

Equifax Inc. (NYSE:EFX) is the leading provider of information and services for consumer financial transactions. Employing more than 12,000 people throughout North America and the United Kingdom, Equifax's information services and systems help its customers grant credit, insure lives and property, authorize checks, process credit card transactions, control health care costs, market products and complete other transactions that benefit the economy, business and consumers.

In our financial information business we maintain, in conjunction with our system affiliates, a national, automated database of personal financial information subject to the protections in the federal Fair Credit Reporting Act, applicable state law, Federal Trade Commission and other applicable regulatory guidance and the industry's and Equifax's own privacy and fair information practices.

In our health record businesses, Equifax has handled health record data for many decades -- and always with special care. Equifax health information services include:

- obtaining and delivering medical records of individuals for life and health underwriting and claims purposes;
- interviewing individuals about health in connection with life and health insurance applications;

- o auditing hospital bills to determine the accuracy of charges;
- o collecting past due patient bills for physicians and hospitals;
- o conducting health exams on individuals applying for life and health insurance.

In carrying out these activities, Equifax follows company-wide fair information practices developed in the 1970's and expanded, refined and restated in 1993 as "The Equifax Information Privacy Code." These fair information practices surpass current legal requirements in the privacy area.

One of Equifax's major goals is to be the preferred steward of consumer information. We recognize that to earn the public trust, we must gather, store and transmit individual health information competently and confidentially only to parties with a legitimate need to know.

In the past two years, Equifax has moved aggressively to apply its knowledge and experience in information management to provide administrative and analytical services in health care. Today, for example, Equifax business units process millions of medical claims for employer health benefit plans, health insurance, and provider network programs. Equifax analyzes data on millions of medical claims to evaluate benefit plan performance and cost.

Now that health care reform has been launched, new information and privacy issues are quickly emerging. Reform initiatives call for provider performance and quality measurements, and more

efficient administration. In part, the success of these and other initiatives will result from the automation of health care information; computerization of patient records; electronic medical billing and claims payment; and greater aggregation of individual health information for important purposes such as outcome analysis, research and health care management.

Simply stated, personal health information will be more accessible and available for more uses. Privacy concerns will require that proper safeguards be established and strictly followed.

CHARACTERISTICS OF CURRENT HEALTH CARE INFORMATION SYSTEM

It is widely recognized that the existing health record information infrastructure is a disjointed, dysfunctional patchwork of databases and systems. Health record information is generated at each encounter with a health care provider. Customarily the event is captured in a partly manual, partly automated format. Biographic information, financial information and sometimes basic diagnostic and treatment information may be automated while detailed medical information persists in a manual format.

Medical records tend not to be comprehensive in that each provider maintains its own records and those records seldom contain all of the information held by other providers who have treated the patient at different times for different problems and perhaps in different cities or states. These records are maintained by

physicians, by a variety of institutional health care providers including hospitals, clinics, nursing homes and less traditional and emerging health care organizations such as HMO's, PPO's and an alphabet soup of new provider arrangements.

Of course, patient record information is also held in non-provider settings such as insurers, government agencies, employers which administer or otherwise participate in insurance plans, and medical researchers. In addition, in an effort to capture, analyze and move a mountain of important data and sometimes paper, a critical industry has emerged, of which Equifax is a part, to assist providers and payers. These organizations provide critical information services, including evaluation, measurement, auditing and health management services.

Overlaying this patchwork infrastructure is a diverse and conflicting array of state and federal law. The handling of health record information is heavily regulated but not in a comprehensive or consistent manner, and generally, not on the basis of the content or uses of the information. Instead, state law regulates on the basis of where the health record information is housed. Health care providers must handle information based on one set of rules. Often even these rules vary materially depending upon the type of health care provider. Physician rules differ from rules for hospitals and other institutional providers while insurers, researchers, government agencies, employers are each governed by different rules even though handling the very same information.

The confusion is compounded by the fact that the law changes each time that health record data cross state lines. Federal law is yet another source of potential conflict. Combine all this with a lack of uniformity in data formats, protocols, nomenclature, operating systems, and virtually every other key part of the process and there is no wonder that the existing information infrastructure is blamed for excessive cost, delay and confusion in the health care delivery and payment process. In this regard, we applaud the effort in H.R.3137 to emphasize the need for integration and uniformity.

It is therefore understandable that leaders in the President's Task Force on National Health Care Reform have called for uniform national rules in the privacy context. They have said:

> Health care institutions, insurance companies, and self-insured employers who transmit health information through interstate commerce often do so without clear guidance regarding which state's laws govern or which state's courts have proper jurisdiction to resolve disputes that may arise. Without the ability to know and to rely on uniform privacy regulations, patients may lack the basis for meaningful consent to disclosure of information. Lack of uniformity of privacy protections may adversely affect the integrity of health data, and the quality of care itself, by undermining efforts to automate health records. These detriments of state-by-state privacy protections will only be magnified in a new health care system where patients would be entitled to coverage anywhere they live in the country and where information for monitoring quality and cost-effectiveness will be collected nationally under the auspices of a national health board. Consequently, many persuasive reasons exist to adopt a uniform federal privacy policy that transcends state borders.

Gostin, et al "Privacy and Security of Information in a New Health Care System," Journal of American Medical Association, November 24, 1993 at 2490.

INFORMATION CHARACTERISTICS IN THE NEW HEALTH CARE INFORMATION INFRASTRUCTURE

Regardless of whether there is comprehensive healthcare reform, a new health care information infrastructure is emerging. Undoubtedly, the new infrastructure will be based on provider quality measurement, an automated health record and a telecommunications system or systems to move information to authorized users. The new, automated health care record will be used for medical decisions, payment decisions, research decisions and health care management decisions. Of necessity, the record will include biographic and demographic data, medical data, social (family) data, financial and insurance data, employment information and other sensitive personal information.

In reforming the nation's health care system this Congress has an opportunity to restructure the health care information infrastructure in a way that maximizes the utility of the health record while protecting personal privacy. In the remainder of my testimony let me identify and highlight some of the key characteristics of a health care information system and some of the key privacy and fair information practice safeguards.

CRITICAL INFORMATION SYSTEM AND PRIVACY ISSUES

WHAT USE, WHAT DATA, WHAT SOURCE

"What use, what data, what source" are the threshold issues and the key issues in any effort to structure a responsive and responsible information system.

Information systems must be user driven. For an information system provider, the key to marketplace success is to design a system that is responsive to user (customer) needs. On a national basis the key to an efficient, cost effective system is to identify all of the legitimate users, understand their information needs and design the system from both a content and an operational standpoint to meet those needs. The information systems that will serve the nation's health care needs, will serve numerous and different types of users. Given this multiplicity and diversity, these systems undoubtedly will feature large, heterogeneous and highly segmented databases, and a flexible, interoperative architecture.

The sources of data for health record systems will also vary greatly from highly technical provider input, to more informal patient input. Given that the reliability of the sources will vary, systems must be designed to identify data based on source and to include merge and purge routines and various internal logic and proof protocols so as to safeguard the integrity of the data.

UNIQUE IDENTIFIERS

One of the difficult challenges in the type of personal information systems that will serve the health care system is matching the right data with the right person. The number of people covered by health data systems and the number and variety of data furnishers will compound the problem. The President's Task Force makes a reasonable point in our view, in recommending a unique national identifier.

DECENTRALIZATION AND UNIFORMITY

As discussed earlier, numerous personal health information databases currently exist and more are being created. It would be expensive, inappropriate and, counterproductive to supplant these databases with a centralized database or even several regional, centralized databases. H.R.3137 takes the correct approach in assuming that there will be numerous and different information systems that will comprise the health information infrastructure and in mandating standards for the interchange of information among these systems. Decentralized information systems for health care will minimize problems with data quality and privacy while taking advantage of available resources.

In a distributed database environment, however, it is critical that there be uniform national data and transmission standards. These standards should cover billing, claims, enrollment, and

eligibility, as well as protocols for capturing medical, financial, insurance and other personal information. Uniformity will not only facilitate the transmission and use of information but also reduce costs, improve reliability and promote consumer use and understanding of the system.

SECURITY

A decentralized and distributed database architecture also puts a premium on security. Security, of course, refers to the ability of a system to protect against unauthorized access to and/or use of data in the system. Security includes technological safeguards, administrative safeguards, personnel safeguards and physical safeguards. Obviously, we cannot in this testimony treat the subject of security in any detail. It is certainly a subject that Equifax has given enormous attention to and devoted significant resources to in both our consumer and our medical information systems.

As I am sure the Subcommittee is aware, there have been several recent and highly publicized breaches of security in health record systems including a sensitive oncology personal record database at the Sloan Kettering Cancer Center in New York. In restructuring the national information infrastructure for the health care system, national, mandatory, state-of-the-art security standards will be necessary, such as standards for audit trails and data encryption.

PRIVACY

Equifax has taken the lead in creating stringent privacy procedures for the handling of individual health record information. However, Americans remain concerned about the privacy of their health information outside the direct care-giver community.

In 1993 Equifax sponsored a nationwide, scientific health information and privacy survey by Louis Harris & Associates with noted privacy expert Dr. Alan F. Westin from Columbia University as academic advisor. The survey results provide the nation with clear indications of what the American public, health care leaders, and government officials involved with health activities consider to be appropriate standards and procedures for safeguarding the privacy and confidentiality of individual health information.

As with the results of earlier Equifax/Harris surveys on personal privacy issues (1990-1993), Equifax is using the findings and insights from this survey to adjust and enhance its health information practices. The 1993 health information privacy survey found that 83% of the public and 93% of health and government leaders believe it is important that organizations reviewing individual records in order to analyze treatments, results and costs should "have detailed privacy and confidentiality policies."

Equifax has internal task forces and outside experts diligently working to apply the company's existing fair information practices to the expanding applications of information technologies

in the health care field. Health information privacy and fair information practice principles should include standards for collection of information; internal use of data; accuracy of information; disclosure of information; and participation rights by data subjects including access and correction rights. A health information privacy plan should also include employee training programs and penalties for employee misuse of health record information up to and including dismissal.

The 1993 Equifax/Harris health information privacy survey also found that 61% of Americans have concerns that their "medical information is being seen by many organizations beyond those that need to see it for health care services." Further, the survey found that 56% of the public and 57% of health and government leaders favor enacting "comprehensive federal legislation that spells out rules for confidentiality of individual medical records."

Equifax shares this public sentiment that strong and well-defined federal legislation is needed to set national standards and provide the legal ground rules for the collection, storage and delivery of medical record information. We look forward to working toward legislation that appropriately balances safeguards, access and uses of individual health information.

HEALTH DATA ORGANIZATIONS

The national information infrastructure should be a private and public partnership. As noted earlier, numerous private organizations are already in the business of collecting, databasing, using and disseminating health record information. Health care reform should build upon these resources. We should not depart from American traditions of entrepreneurship and marketplace freedom by licensing or otherwise attempting to restrict database activity. It should be noted, however, that the Equifax health privacy survey found that 94% of the public and 97% of leaders feel that when government, insurers, and employers select information processing companies to do medical claims processing and health data analysis, the selection should be "on the basis of a proven record of protecting the confidentiality and security of the personal records they handle." We urge the Congress to encourage health record information users and consumers to follow this approach.

CONCLUSION

In conclusion Mr. Chairman, Equifax believes that effective information systems are imperative if health care reform is to be successful. While the technology exists the necessary standards for interconnecting systems, exchanging information and protecting

data remain to be developed. Realistically, this process will be time consuming.

Equifax welcomes the opportunity to share our expertise with the Congress and the Administration on both the technical and privacy aspects of developing health care information systems. We look forward to continuing to work with the Congress.

We thank you for this opportunity to testify.

Mr. SAWYER. Thank you both very much. You have helped to focus the discussion based on the real experience that you have both had. I am sure that you both will have plenty of opportunity to contribute to this process as we go forward.

Let me just summarize the kinds of questions that I asked the previous panel. How do we go about quantifying the cost and savings of assembling all of the diverse parts of a system of this kind?

Mr. RAHIYA. I think I will let my colleague tackle that one.

Mr. SAWYER. No, the way you do it is you say there are five essential ways to do this, and he will list them. [Laughter.]

Mr. RAHIYA. Well, just one comment. There have been numerous studies, and some were referred to in earlier testimony. You have to study the studies to find out if anybody really has put a handle on it.

But I do think there are some good studies that have been conducted within the last year that come close to what the number and numbers would be. Assuming that they are 80 percent accurate, we should move on with the task at hand, just assuming that it is going to be immense and then doing it correctly so there are savings that fall out down the road.

Mr. TISDALE. I would agree that there has been some excellent work done, primarily in quantifying the administrative savings that can be garnered. However, for the lack of data, we run out in what the potential savings are in the benefits and utilization side of the equation. It is a far larger bubble.

Obviously much of our estimates today have been extrapolated. I think you can look to some examples within private industry where components of the overall information infrastructure are already being delivered to learn what the cost aspects of some of those are. Some of those may be something of a particular technology like a network, or they may be an individual organization's investment. For example Kaiser recently estimated that they would spend upwards of a billion dollars in capital over the next several years in information technology infrastructure, and yet they represent a fairly sophisticated delivery system.

So I think you can look to both examples of existing technology and existing health care business investments, to help quantify it.

Mr. SAWYER. Clearly it is fair to say though that regardless of the billions that may have to be spent up front, that the immediate and foreseeable savings far outstrip the potential costs of initial investment.

Mr. TISDALE. That would be correct, particularly if you lean toward use of the existing infrastructure as much as possible and realize that what we are asking you to do is through the use of standards and technology policies, to allow those communications systems or that data to be passed from different pieces of the system to each other, rather than actually building something from the ground up.

Mr. SAWYER. Right. Mr. Rahiya.

Mr. RAHIYA. Mr. Chairman, in most of our experiences we have evolved from a paper environment to a technology and a database environment. The data source usually starts with some paper document. The road from paper to technology, where you finally get the leverage and the benefit of information technology is long and ar-

duous. There is usually a lot of debris in the wake, and many times the tunnel is so dark for so long you wonder if you will come out.

But when the paper environment has at last been automated, the benefits to all concerned, whether it is the person about whom information is gathered, or the various users of the information, the benefits seem to spill down to all in geometric terms relative to what the investment was in bringing the system about.

But the conversion process is long and tough. If the goal is in sight, it is certainly worth it.

Mr. SAWYER. With so many players in such a system, how do you begin to ascribe costs and divide them among those who will have to contribute to building the system? That includes the federal government, states, providers, a whole range of players in a complex, mixed system of this kind.

Mr. TISDALE. I think part of the issue is to help describe the value of the system to the different players, as well, and in many cases through private enterprise that will create the contribution. An example might be that the electronic medical record, if viewed as an expensive claim collecting technique, will not be well received in the medical community. If viewed for its value in terms of the clinical setting, in terms of analysis or prepping for patients, triage, whatever it might be, then there will be a willingness to contribute capital to the electronic medical record as an aspect of technology.

Mr. SAWYER. Sure. How long is this going to take? We are sitting here trying to build timetables into legislation that fits with comparable or related time tables in a variety of different reform proposals. It seems to me that to the degree that each of those reform proposals may depend on this central nervous system, that this may be a controlling element in achieving the goals no matter what reform it ultimately fits with.

What kind of message should we send about not only large scale time tables, but the way in which it will vary among different kinds of data sets and uses to which that data will be placed?

Mr. RAHIYA. A long time. [Laughter.]

I do not think I am able, obviously, to put a number on it. It will take years. It will take a lot of years. It is so important that benchmarks be established so goals can be accomplished along the way, much like in a football game. A first down can be a wonderful goal to have because it moves you toward the goal line.

The mega solution, as a goal, will be an unattainable goal because no one will ever be able to put their arms around it. It is going to take years to do. If it is done in some bite size pieces where people will not lose their resolve to stick with it and, in essence, move the ball down the field, it will take place. But, it is going to take a long, long time.

Mr. TISDALE. I would say that there is probably not a finite time table that anybody can predict, and I think the answers of the other panel were in the ball park of what it might be.

I would agree with the earlier observations, as well, that probably the greatest way in which the Congress can help us in private industry rise to the occasion, as well, is in the establishment of standards—data definitions and protocols that will be used.

Those are the barriers that today often get in the way of even delivering the technology that can be brought to bear.

I would also say, don't underestimate what might be characterized as more the emotional side of it. The issue of rights of privacy and confidentiality could absolutely stop a lot of the work in its tracks if not resolved up front.

Mr. SAWYER. Clearly this is a game that does not have a fourth quarter. It will continue. Will we know when we are ready at least to begin?

I mean I am concerned that those who would argue that somehow we do not need to do all of this or that they are afraid of doing all of this will let the perfect or the final or the complete become the enemy of measurable progress. A long time, whatever that is, is maybe how long it takes until it becomes so routine that we do not really think about it, but the process of starting really has got to be compatible with the process of reform.

Would you suggest to us that that is possible and feasible?

Mr. TISDALE. I would suggest it is possible. The time line is certainly a longer one, but an analogy might be all of our experience, say, in banking and financial services. Each of us, probably through paper transactions at the counter, did our banking at an individual bank for many years. Then you had the emergence of the ATM-style industry that began to create regional access using electronic interfaces and now international access.

I do not think we are looking at what it took, the 20 years, say, to go from paper to international banking electronically.

Mr. SAWYER. We have learned a lot from that process.

Mr. TISDALE. And a lot of it is leveragable. A lot of it will be the infrastructure that is, in fact, used to support health care today. I would also argue that there is a lot of what we need to do being enacted in different places, but it is the type of investment today that often will have to be redone, adjusted in several cases, because the investments are being made in unique, proprietary, technological and business designs today.

Mr. RAHIYA. I think picking the immediate end states to reach, knowing that it is an evolution, is a challenge. In our business when we think we get to an end state, we are never there because it is always evolving. Either new technology shows up or new uses show up or some part of the formula changes.

There might be a lot of value, and I know that an immense amount of work has been done on the computerized patient record. If that is the source of the information, when either rolled out or rolled up, whatever is appropriate, there has to be a uniform source, to start with.

That does not mean things will malfunction without it. If there is a data source that is accepted by all, what is here is good information, it can help lead to the measurement of the quality of care. It can help lead to the measurement of patient satisfaction. It can help to lead to the measurement of physician or hospital performance.

This type of information, needed to begin to control and manage the business on a more global scale, where we will understand what is going on in health care, would be one way it could start to work. There has to be some unified data with which to start. Now it is so diverse and scattered that you can only address it in little sections.

You can go into a hospital and measure it, but if you try to measure a community or try to measure bigger things, it takes all of the king's horses and all of the king's men, and people give up.

Mr. SAWYER. You have both touched on this really when you have talked about confidentiality and the management of the security of a system, as well as the utility to which that information can be put. Let me go back and ask those three basic questions again that I asked the others.

What is the repository of such a core of information? Who is the owner? Who is the user, to go back to the notion that it is user driven?

Mr. RAHIYA. The issue of users depends on the specific health care information. There can be many legitimate users. The patients certainly have rights, as do physicians and the administrators in hospitals. When we come to the reimbursement piece, if an employer is involved, they are going to see part of it. If it goes to an insurer, they are involved.

We must start with the premise that with health care information a lot of people have a legitimate right to see it, because they are either involved in the care-giving, the financing or the administration.

With the ownership issue, what we have found over the years, is it is not much of an issue because so many parties have a right to the information. What is important and what we have found in our business is that we have to protect the privacy of the individual, as well as secure the information from people who have no need to see it and have no need to access it.

Our accesses are based upon need to know, protecting it all the time, even within our company. Individuals do not have access just because they are interested.

Ownership tends not to become an issue. We have never really worried about that because different people have different uses. If we protect it like we know we should, then it tends to work very well.

Mr. TISDALE. I think I would agree, with some parallel observations. In a given setting, for example, and one I can point to is, say, Harvard Community Health Plan in Massachusetts—you have different degrees of access based on need. So not everyone working in a clinic has the right or the ability to access the entire medical record.

I further agree that it probably is somewhat of a misrepresentation to suggest that you are going to continue to aggregate everything about the individual into one physical location or into one computer bank, if you will, and then that is the physical point at which everybody will access the information to get just the piece they need.

I think it is probably more appropriate to suggest that there will always be slices of the information that will be needed by different users and that they will have access to those in different ways, that they will restrict them, and that, in fact, the slices themselves may reside in different physical locations, which further promotes or supports the issues of security and privacy.

Mr. SAWYER. The public perception of all of this, your ability to actually produce a system that, in fact, assures a greater degree of

security than present paper-driven systems do, is something in which I have a great deal of confidence. The ability to give comfort to a nation that that is in place is another matter entirely.

Can we talk about, can we describe in publicly usable terms the ability that we have to mask data, to assure its anonymity in assuring access to researchers and to others, public health officials, who deal broadly with the overall condition of health in a community, as opposed to individual medical records and the health of a person?

Mr. TISDALE. I think the answer is yes. I think, again, different organizations or medical groups have even for their own reasons taken cuts at that just to run their internal operations today, but I think some of that exists and can be lifted.

I think it is not to be underemphasized though that the public needs in many ways to feel that they are the ones who control each type of access or each style of use of the information about them; they want to control that access and that privacy by decisions they have made. I would say that the technology will certainly allow the elections that that individual has made to be reflected in a system that then can control the access to that data.

For example, an individual may be very comfortable with their entire medical record with their name or identification number on it being available for certain use or they may feel that they would like their medical information to be used only in a sanitized manner with no reference of identification. If they have that choice, the technologies will allow us to use that data in that way.

Mr. RAHIYA. On the medical information side, as that information moves away from the patient and physician relationship, access must become more stringent and the amount of information may become less detailed and less specific.

Obviously in the care-giving setting, physician and patient together, everything is known or should be known. As information moves into the payment process, into further evaluations, if it is rolled up on a community basis, or as Mark mentioned in State organizations, then it is important that those who have access get access to limited amounts of that information. It is not easy to implement, but it can be done.

And, again, if I can go back to how we deal with this information, we are fanatical about the privacy of the information that we maintain in our databases. It is our culture. We have had to be that way because the databases we are talking about are repositories. Organizations put data in for the benefit of later getting out information in aggregate. Then they can see things they could never see by just looking at one record or one data set. It has to be worked through and evaluated because certain individuals may not need everything that a physician has to see. That is the structure you have to put over it. It is an access structure, the what data, what source, what use that I mentioned earlier.

Mr. SAWYER. The analogy that I am probably most familiar with is the equally fanatical commitment to confidentiality over many years that the Census Bureau has devoted to its information, and the assaults that have been made on that information are not so much through surreptitious means, but through the courts in order

to make use of that data for law enforcement purposes and other matters of governance and administration.

It has been held sacrosanct, but it has yielded a system that is quite separate and apart from all the other data and can be used in a variety of creative ways, but certainly the kind of interactivity among uses that would be required of a health data system is much more complex than that.

I am not sure that I am going to come to a question with all of this, but it is a concern that I think we need to continue to explore. Let me offer an example.

With all of the discussion, for example, in recent days about the application of technology through the FBI and other law enforcement to do transactional analysis of human behavior based on simple administrative records of billings. It has demonstrated a profound capacity to identify and isolate individual transactions and to analyze for substantive purposes.

As we all become more familiar with those kinds of techniques, are there ways to assure that, for example, the kinds of billing records, and to think of a naive example, I guess a diabetic who is concerned about his public awareness of his particular condition. It would be fairly easy to track from virtually the kinds of medications that he used.

Mr. TISDALE. You are describing a complex problem.

Mr. SAWYER. I am concerned about not just the medical record, which of course we all understand, but the transactional records that flow from that condition that may be precisely descriptive of what that condition is even though it is not intended to be.

Go ahead.

Mr. TISDALE. I was going to say that you may have, in fact, in the individual pieces of that person's life style properly adhered to whatever handshake or formal agreements of privacy or confidentiality existed for each of the components or steps along the way. It is when you assemble a life style that the individual sometimes becomes very anxious that this is able to be done, in some cases without violating any individual sense of agreement along the way.

Mr. SAWYER. That is correct. It is the product of the patchwork, not any breach of faith among responsible professionals at every step of the way.

Mr. TISDALE. And in health care you could argue that the leap might be as you move more from treatment outcomes data, more to life style, wellness and prevention that you begin to draw in community or societal or individual pictures of life style that influence health care.

Mr. RAHIYA. One way to address that is the organizations that are in the stream of personal medical information, from the patient-physician relationship, through the organization to the financial piece, and so forth and so on, have to take upon themselves a goal of having fair information practices with a big, big emphasis on privacy protection.

It will be protected if the culture of the organization that is handling it understands that they have to be sensitive to that information. For example, suppose a claim paying shop is very cavalier while they are just processing claims, and allow stacks of information to lay around where anyone can observe them. To know that

someone is taking Prozac, or a similar drug, may suggest a mental health issue. Well, that is wrong, however you cannot put it all behind iron bars. The people handling such information have to be trained. They have to be coached. They have to understand what is going on. They have to sign confidentiality statements with respect to the information they handle.

Although it is very routine, you are passing through all types of information, which if it ever were made public, it would be people's health history.

So I think, Mr. Chairman, that one of the ways to address this is that organizations have to have these policies of privacy protection. It cannot simply be, sure, we do it, and now let's go to lunch. It has to be an overriding concern when information that is that sensitive is being handled by many different people.

In the paper environment it is even a bigger problem, than when that information finally moves into a technology stream.

Mr. SAWYER. Thank you both very much. I am certain that we will be turning to you in written forms and in other formats to ask for your assistance, as with those who were represented in our previous panel this morning.

Your contributions to this work are just going to be invaluable, and we look forward to staying in touch with you.

Mr. RAHIYA. Thank you very much.

Mr. TISDALE. Thank you, Mr. Chairman.

Mr. SAWYER. If there is no more business to come before us today, we stand adjourned. Thank you.

[Whereupon, at 12:00 noon, the subcommittee was adjourned subject to the call of the Chair.]

H.R. 3137: DATA NEEDS AND RELATED ISSUES FOR IMPLEMENTING HEALTH CARE REFORM

WEDNESDAY, MARCH 16, 1994

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CENSUS, STATISTICS
AND POSTAL PERSONNEL,
COMMITTEE ON POST OFFICE AND CIVIL SERVICE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:45 a.m., in room 311, Cannon House Office Building, Hon. Thomas C. Sawyer (chairman of the subcommittee) presiding.

Members present: Representatives Sawyer and Petri.

Mr. SAWYER. It's not so late that I can't still say good morning and thank you for your patience. Today is our second hearing about the national information system that may well be central to successful health care reform.

At the first hearing we talked about the goals for that system, how it might work in practice, what the appropriate federal role might be. Clearly, the primary uses for that system include paperwork reduction, detection of fraud, and, perhaps most importantly, the timely transmittal of medical information.

A secondary use, of course, is for research and statistical purposes in a broad array of fields, but none more important than the management of public health, which will be central to successful health care reform in the first place.

It is clearly important to understand those uses before we design and implement a system. If those uses will benefit society, we ought to accommodate them, and we want to talk about how to accomplish that goal.

Our discussion today talks about the benefits and the risks of providing access to that kind of information. We need to strike a balance between individual privacy, in the confidentiality of information, and responsible access for research and other scientific purposes on the other.

First, we need to realize that the very real concerns of Americans about privacy are paramount. A lot of data have been collected to demonstrate that Americans simply feel that their medical histories represent the most sensitive information that exists about themselves. They don't want their employers or anybody else to be able to get at that information. They perceive technology, not as a benefit to that kind of privacy, but a real threat to it. They fear losing control over their own medical information.

The truth is that they have very little control over their records today. The current system leaks like a sieve. They don't own the

information. They are often denied access to that information, even denied permission to view their own records in some cases.

We need to view this reform as a fresh opportunity to address these kinds of issues as well. There are all kinds of examples of existing unauthorized disclosure, one horror story after another. One in particular came to my attention, that of a Colorado medical student who sold information to malpractice attorneys at $50.00 a record. Now, that may reduce the necessary government subsidy for medical education, and that's important, but that's not the way to do it. The problem is fairly widespread.

The Office of Technology Assessment's findings raised two key questions that bear on our discussion today. Who has been primarily responsible for those kinds of documented problems, and will a technologically driven information system create a greater potential for increased disclosures or provide protection?

It seems to me that most unauthorized disclosures occur from the inside out, that is, among people who already have legitimate uses for the information. In that sense, it cannot be more insecure, but technology has the potential to create a more secure system.

I hope that today's witnesses will help address those kinds of questions.

The second key issue is the benefit of providing access to medical information. There is enormous value in allowing well-defined access, but Americans have got to have confidence that that access is carefully controlled. The goal is for all medical professionals to have necessary information as part of diagnosis and treatment of illnesses, and information about an individual is critical in those cases.

But, an individual's identity is not necessarily of primary interest for researchers who look for patterns and trends and probabilities, in order to analyze and seek common characteristics. That kind of research takes place today. It has a direct effect on national policy. Access to a broader range of information, more carefully defined, can even do more good in terms of existing scientific projects and new ones that more sophisticated access to information might make possible.

Striking the right balance between privacy and access is not going to be easy, but that's really what we are here to talk about today, and I am pleased to welcome our witnesses.

Before we begin the first panel, if I could excuse myself for a moment, I have a telephone call from my chairman, and no matter what you are doing you always take a telephone call from your chairman. I'll be right back.

[Recess.]

Mr. SAWYER. Thank you for your patience. I just went through an opening statement. If you'd like to offer observations——

Mr. PETRI. A very brief one, thank you, Mr. Chairman.

Mr. SAWYER. Then we can get on with our business.

Mr. PETRI. I'd like to thank the panelists for being here this morning, and my only comment or observation is that this is actually, the subject of today's hearing and the one we had a week or so ago, is one aspect of a major social issue that actually is being answered in the marketplace, I guess. As one goes to the grocery store and pays with a credit card and then you get the individual

items on your sales slip and the bill turns out, those companies can, and do, sell information on people's buying habits.

I know that companies in my district who deal with Walmart, for example, are impressed that Walmart now deals—uses its sales data as a profit center and will sell it out into the marketplace to entrepreneurs to try to identify niches, people's buying habits in different areas, or different types of things. So, the ability to massage and have information about individuals is rampantly increasing in our society as computerization becomes more pervasive, and it's something that's not restricted to health care, it goes beyond that into all aspects of our existence as we engage in transactions with various people that are recorded electronically.

So, I don't know if that's a helpful observation or not, but I do think that some of the issues that we are wrestling with in this area are actually much broader than just health care, and have to do with how we try to balance the economic advantages of an open society and free exchange of information with individuals' rights to have some of their details of their daily life kept with some measure of privacy and discretion, not misused.

So, again, thank you for being here today, and we look forward to your testimony.

Mr. SAWYER. Thank you.

Let me welcome our first panel. Our first panel is Nan Hunter, who is Deputy General Counsel of the Department of Health and Human Services. She is joined today by Doctor Roz Lasker, Steven A. Pelovitz, Doctor John Silva, and Katherine K. Wallman. If you'd like to identify each of them further for the record, please feel welcome to.

Let me emphasize that it is not necessary to share the total text of your testimony. The entire written testimony will be included in the record, but you should feel free to emphasize, and summarize and focus our attention as it will serve your purposes best.

Thank you for being here.

STATEMENT OF NAN D. HUNTER, DEPUTY GENERAL COUNSEL, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES; ACCOMPANIED BY DOCTOR ROZ LASKER, M.D., DEPUTY ASSISTANT SECRETARY FOR HEALTH POLICY DEVELOPMENT, U.S. PUBLIC HEALTH SERVICE, HHS; STEVEN A. PELOVITZ, DEPUTY ASSOCIATE ADMINISTRATOR FOR MANAGEMENT, HEALTH CARE FINANCING ADMINISTRATION, HHS; DOCTOR JOHN SILVA, M.D., PROGRAM DIRECTOR, ADVANCED RESEARCH PROJECTS AGENCY, DEPARTMENT OF DEFENSE; KATHERINE K. WALLMAN, CHIEF, STATISTICAL POLICY OFFICE, OFFICE OF INFORMATION AND REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET

Ms. HUNTER. Thank you, Mr. Chairman, Mr. Petri.

I'm pleased to be here this morning to discuss the information aspects of health care reform, and the relationship between privacy concerns and research needs.

I would like to begin by just introducing my co-panelists, Doctor Lasker from the Public Health Service, Steven Pelovitz from HCFA, Doctor Silva, who was co-chair of the Information Systems Working Group for the President's Health Care Reform Task Force,

and Katherine Wallman, who is the Chief of the Statistical Office of the Office of Information and Regulatory Affairs at OMB.

I'm going to present a summary of the testimony, and my co-panelists and I will divide up any questions that you might have.

The potential benefits of an effective information system under health care reform are enormous, and I think it's important to start at that beginning to emphasize that. Consumers would be empowered by this information to make wiser and truly informed choices about providers and health plans. Doctors and other professionals will be able to coordinate care and make better treatment decisions. Medical outcomes research would be vastly improved. Public health systems would be better able to protect all of us against disease and injury. We would be able to better detect and prosecute fraud and abuse. And, lastly, we will be able to reduce the excessive paperwork that is now drowning both professionals and consumers by using one uniform claim form.

Moreover, reaping the benefits of better health information does not require, necessarily, a big government approach or the creation of new technologies. Most of what we need already exists in both the public and the private sectors.

Remarkably also, there is a widespread and bipartisan consensus on the key features of what a new system would look like. For example, Mr. Chairman, the bill that you introduced with Representative Hobson and Senator Bond, reform proposals introduced by Representative Cooper, and Senator Chafee, and the President's Health Security Act, all support a national framework for health information that includes several key features in common.

First, uniform data standards. Under the President's bill, selected data items related to enrollment, claims for payment and encounters with health care professionals will be recorded in a nationally uniform format, either on paper or electronically.

Second, a unique identifier number for individuals, providers and health plans. Under the President's plan, each consumer would have a Health Security Card, and with a swipe of this card most paperwork would be eliminated for consumers.

Third, an electronic data network. Health plans will maintain electronic documentation of all clinical encounters for their enrollees, using data that conformed to the national definitions and standards. Alliances will maintain electronic enrollment files for all of their eligible residents, and selected data items reported by alliances and health plans will be collected, compiled and transmitted by regional data centers.

And, fourth, strong privacy and security protections to keep sensitive health information confidential. We are committed to achieving better and more uniform safeguards to protect privacy. With the exception of federal agencies covered by the Privacy and Public Health Service Acts, legal protections for health care information today are variable and often inadequate. Americans expect and are entitled to careful confidential treatment of information about their health.

Privacy protections are, therefore, an integral part of the Health Security Act, and need to be, both to protect individual rights and to assure the quality and accuracy of information in the health care system. Privacy protections are even more important as we move

toward computerized nationwide health information networks. To realize the benefits of such networks, including those related to research, safeguards are needed to ensure that individually-identifiable information is used only when truly necessary and not in ways that will harm individuals.

The administration believes that confidentiality controls are essential. Under the Health Security Act, medical records would be far more protected from inappropriate uses or disclosures than they are today. The Health Security Act creates a framework for a comprehensive national policy for protecting confidentiality of health information. The details of those protections are set forth in my written testimony, and I am not going to go through them in this presentation.

But, I want to move on specifically to the issue of research. This new system will provide unprecedented opportunities for many types of research, including clinical outcomes, epidemiological, health services and policy research.

The question then is not whether the information in a new network would be conducive to meeting many of the research and statistical needs of the nation, but whether this information can be made available to researchers in ways that protect confidentiality. We believe that it can.

Let me distinguish two types of situations. Most statistical research needs can be met without compromising privacy at all, through the production of what are called public use files that are stripped of all individual identifiers and any other information through which individuals could be identified indirectly or directly.

Although statistical analyses and research often require linked, person-level information, and also, although unique identifiers are required to create such files, the researchers performing the analyses do not need to know the identification of the particular individuals from whom the information was obtained.

Both the Medicare program and the National Center for Health Statistics have excellent track records in creating such public use files, and making them available to qualified researchers.

Some research does require access to individually-identifiable information. In general, we believe that disclosures from the network of individually-identifiable information, for the purpose of research, should occur only when the individual has given consent for such a disclosure.

In many studies, individuals can have the option to participate voluntarily. In other cases, strict standards and careful review, including by Institutional Review Boards, are needed to ensure that no alternative to the use of individual identifiers is possible, that only the minimum amount of information necessary to carry out the study is released, and that stringent penalties are imposed for any misuse of data by the researchers.

All non-operational uses of individually-identifiable data should be considered only in the context of carefully reviewed and approved research protocols.

One way to implement the legal protections for privacy of data used in research would be through the Regional Data Centers. Regional Data Centers, which could be public or private, and configured in a number of ways, can serve as research and statistical

centers with some of the same legal protections as the Census Bureau. There would be a number of data centers, all of which could be immunized from the scope of reporting laws and judicial process, just as the Census Bureau is.

The obligation to report diseases or to furnish records in a court proceeding would continue to apply to the individual provider, as is the case today, but we are considering and discussing options for shielding these new clusters of health information created in the new system from that kind of access by the government, along the lines of the recommendations of the Institute of Medicine in its recent report, Health Data In The Information Age.

For their research and statistical functions, the Regional Data Centers would link enrollment, encounter and other data and perform the necessary work to remove individual identifiers before releasing data to researchers. Stringent penalties would apply to all persons who worked in the Regional Data Centers and to all researchers who obtained data from them, to prohibit and punish anyone who improperly revealed individually-identifiable information, or who received public use files and then attempted to reidentify individuals in any manner.

As a final note, I would like to add that access to information in the network by other statistical agencies may be appropriate, such as access to enrollment data, not medical data, but enrollment data by the Census Bureau. In this instance, existing statutes and longstanding practices governing the Census Bureau have successfully prevented invasions of privacy.

Moreover, the benefits of these institutions, again, the Census Bureau securing access to data in the new system, would be substantial. Access by these agencies could either be determined appropriate by the National Health Board or could be clarified in the Act.

Let me conclude by putting the information aspects of the President's proposal in a broader perspective. The Health Security Act will reduce the burden and cost of recording information, while at the same time assuring that all participants have the information they need to carry out their functions and make informed decisions. This system will be surrounded by legal and operational confidentiality safeguards built into the design at the beginning and basic to its operation to protect the privacy of the people it serves.

A combination of legal and other safeguards will offer the public assurance that individually-identifiable information will be used respectfully and carefully, and will make it possible for all of us to benefit from the results of expanded research.

We look forward to working with you, Mr. Chairman, and other members of the Congress, on these important issues.

Thank you.

[The prepared statement of Ms. Hunter follows:]

PREPARED STATEMENT OF NAN D. HUNTER, DEPUTY GENERAL COUNSEL, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Good morning Mr. Chairman and members of the Subcommittee. I welcome this opportunity to discuss the information needs of health care reform and, in particular, to address how the framework for health information envisaged by the Health Security Act will accomodate the research and statistical needs of the nation.

Mr. Chairman, as bills recently introduced in the Congress indicate, there is growing consensus about the features of an effective information system under health care reform. For example, the bill you introduced with Congressman Hobson and Senator Bond, reform proposals introduced by Congressman Cooper and Senator Chafee, and the President's Health Security Act all support a national framework for health information that includes:

- national standards for clinical and administrative data;
- public-private electronic networks for the nationwide exchange of health information;
- unique identifiers for individuals, providers, and health plans; and
- strong privacy and security protections to keep sensitive health information confidential.

At the core of this emerging consensus -- which is not only bipartisan, but also includes most of the stakeholders in the private sector -- is an appreciation that a national framework for health information is critical to achieving the basic goals of reform: choice, quality, security, simplicity, and savings.

Such a framework is needed to provide all participants of the health care system with accurate, comparable, and timely health information. This is of benefit to consumers in making choices about providers and health plans. It enables health care professionals to coordinate care and make better treatment decisions with their patients. It supports research in medical outcomes to identify what works best and how to provide care more efficiently. It provides information to protect the public against disease, injury, and disability. It enables more effective detection and prosecution of fraud and abuse. And it facilitates assessments of access to care, health status, utilization, quality, and costs of care, enabling all participants of the health care system to fine-tune their performance.

A national framework for health information is also essential if we are to reduce the excessive paperwork that is drowning health care professionals and consumers today. Currently, the health care system is collecting enormous volumes of data. But because the same information is reported in hundreds of different ways and local information systems cannot communicate with one another, the administrative burden is great and the information that is generated is not as useful as it could be. To the extent that forms can be standardized -- for example, having a uniform claim form -- and to the extent that enrollment and encounter data generated in the course of operating the system and providing care can be used for other health-related purposes, the health care system can

achieve substantial administrative simplification as well as substantial savings.

Reaping the benefits of better health information does not require a big-government approach or the creation of new technologies. Most of what we need already exists in both the public and private sectors. We can go a long way by facilitating linkages among these existing systems and by establishing a national network of local health information systems that speak a common language.

What we do need, however, and are committed to achieving, are better and more uniform safeguards to protect privacy. With the exception of federal agencies covered by the Privacy and Public Health Service Acts, legal protections for health care information are variable and often inadequate. Americans expect, and are entitled, to careful, confidential treatment of information about their health. A national framework for health information holds great promise in supporting the research and statistical needs of the nation. But to realize this promise we will need to delineate a careful balance between protecting privacy and carrying out important functions.

THE INFORMATION FRAMEWORK IN THE HEALTH SECURITY ACT

The national framework for health information described in Title V of the Health Security Act is actually very simple:

- Health Security Card. Under the Act, every American receives a Health Security Card with a unique identification number. With a swipe of this card, most paperwork hassles are eliminated for consumers. Each provider, health plan, and employer in the system also receives a unique identification number, substantially simplifying their administrative burdens.

- Uniform Data Standards. Selected data items related to enrollment, claims for payment, and encounters with health care professionals are reported in a nationally uniform format, either on paper or electronically. Uniform definitions for these data items and standards for the electronic exchange of this information are developed through a broadly representative process, with input from consumers, providers, health plans, employers, public health professionals, government agencies, researchers, and standards development organizations.

- Electronic Data Network. Health plans maintain electronic documentation of all clinical encounters for their enrollees using data that conforms to the national definitions and standards. Alliances maintain electronic enrollment files for all of their eligible residents. Selected data items reported by alliances and health plans are collected, compiled, and transmitted by regional data centers, which can be configured in a number of ways.

- Point-Of-Service System. In the long term, the Health Security Act could facilitate the development of a point-of-service health information system that collects reportable data items as a by-product of care delivery. Such a system would provide relevant, privacy-protected patient information directly to authorized providers. For example, requests for tests could be automatically forwarded to the appropriate laboratory and results could be returned automatically to the ordering physician. Medical knowledge, national outcomes data, and report card information could be brought to providers and patients during encounters and to consumers in their homes or workplace.

The network technologies we refer to in the Health Security Act already exist and are, in fact, currently in use in the health care community. For example, the current Medicare claims payment system uses electronic networks. An increasing number of electronic claims move along the network from the point of service, to the intermediaries and carriers for processing, to the Common Working File host sites for final adjudication, with the final connection being electronic funds transfer to the provider. Examples are also abundant in the private sector. For instance, the EDI-USA network of Blue Cross plans manages over 600 million claims per year, all electronically. These currently employed technologies can serve as a foundation for building the information infrastructure to support health care reform. However, without national standardization and administrative simplification, the full capabilities of these technologies cannot be realized.

The Health Security Act substantially reduces the reporting burdens that providers currently face while making the information they record far more useful. Providers are currently required to record information pertaining to claims and encounters and will continue to do so under reform. But this will be far simpler under the new system since all reporting will be done in a uniform format (for example, a standardized claim form). Moreover, a national health information network will permit data recorded once to be used for multiple health-related purposes, thereby reducing the burden of duplicative reporting. Since decisions about standardization will be made through a broadly representative process, data items and definitions included on enrollment and claim/encounter forms will be more likely to serve the needs of all participants in the health care system.

PRIVACY PROTECTIONS IN THE HEALTH SECURITY ACT

Privacy protections are an integral part of the Health Security Act -- and need to be, both to protect individual rights and to assure the quality and accuracy of information in the health care system. Without strong confidentiality protections 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 could in some cases lead to falsified information or untreated disease.

Privacy protections are even more important as we move toward computerized nationwide

health information networks. These networks have enormous potential to extend our knowledge base and to provide consumers and others in the health care system with useful information to support informed decisionmaking. But to realize the benefits of such networks -- including those related to research -- safeguards are needed to ensure that individually-identifiable information is used only when it is truly necessary and not in ways that will harm people.

Aside from Federal health record protections under the Privacy and Public Health Service Acts, and national protection of patient information in drug and alcohol abuse treatment programs, legal protections for health information today exist primarily at the state level, and these vary greatly. Only a handful of states have comprehensive health information confidentiality statutes. Many have statutes covering particular types of information (such as HIV infection and mental health information). Some have privacy laws covering insurance information.

The Administration believes that confidentiality controls are essential and under the Health Security Act medical records would be far more protected from inappropriate uses or disclosures than they are today. The Health Security Act creates a framework for a comprehensive national policy for protecting the confidentiality of health information. It includes provisions for protecting the information to be gathered by the new system, as well as, ultimately, designing national legal protections for information held by all health care providers.

There are four principal elements to the safeguards for privacy in the President's bill:

- First, within two years, the National Health Board will promulgate detailed standards for confidentiality of the information in the new system, based on principles set out in the bill.

- Second, there will be controls, with criminal and civil sanctions, on improper use of the Health Security Card or the unique identifying number chosen for the system.

- Third, within three years, the Board will propose comprehensive Federal legislation to protect health information. This will cover, for example, all pre-existing records of physicians and hospitals.

- Fourth, there will be ongoing monitoring and advice from people outside the Federal government to assure that privacy concerns are carefully considered. The National Health Board will have an advisory council on privacy and health data that will include members distinguished in data protection and privacy, ethics, civil liberties, and patient advocacy.

The bill also sets out basic standards upon which the Board will base its rules, none of

which exist today as uniform, national standards for confidentiality of medical records.

- Individuals will always be able to see and get a copy of information about themselves, and they can correct erroneous information.

- Individuals will have a right to know what entities hold or use information about them, and for what purposes.

- Disclosures of individually-identifiable information will be carefully restricted to those authorized by the individual, or for purposes of operating the system, or for purposes meeting criteria established by the Board that are consistent with the general principle that individually-identifiable information is used only when necessary for carrying out the purposes of the Act.

- Disclosure will be restricted to the minimum necessary to accomplish the purpose of the disclosure.

- No identifiable information about an individual will be used to set premiums based on risk adjustment factors, or to make employment decisions.

- Information about patients that is exchanged among health plans, alliances, and regional data centers will use only an identifier number, and not a name, in order to prevent patients from being easily identified by staff operating the system.

- The unique identifier assigned to each individual will not be used to connect individually-identifiable information from the health care system with information outside the system, except when necessary to administer the health program. To require anyone to give his or her number, or to use the number, for any purpose other than the health program, will be a criminal offense, and will also subject the offender to civil money penalties.

- There will be technical and administrative safeguards, such as computer and communications security measures, to prevent unauthorized persons from getting information.

The bill does not alter the existing powers of courts with respect to health care information, nor does it alter existing requirements for reporting disease, child abuse, birth, or death.

RESEARCH AND STATISTICAL USES OF HEALTH INFORMATION

What impact will the national framework for health information and the privacy protections outlined in the Health Security Act have on research?

There is no doubt that 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/claim data will provide a limited number of elements characterizing encounters with practitioners, facilities, pharmacies, and labs (potentially including such elements as diagnosis, reason for service, service provided, site of service, provider, results, complications and charges). Under the Health Security Act, these data will be recorded in the same way for all individuals and all encounters throughout the nation.

Five features make this health information network particularly useful to researchers.

- It provides comparable information that is national in scope and that can be analyzed at any relevant geographic level.

- Individual identifiers permit encounter data in the system to be linked over time. As years of experience with the Medicare information system have demonstrated, these linkages transform "administrative" data into clinically and economically meaningful information characterizing episodes of care or total patient care.

- Individual identifiers permit linkages of enrollment and encounter data, facilitating analyses of utilization, quality, and costs of care in different population subgroups and in different geographic regions, alliances, and health plans.

- Data within the system can be linked with data from other sources (such as national health surveys, vital statistics, treatment registries, and public health surveillance data), enhancing the scope and efficiency of research.

- Enrollment and encounter databases can serve as a sound, national sampling frame for studies of specific conditions, treatments, types of providers, and access to care (such as civil rights issues).

The question, then, is not whether the information in the network is conducive to meeting many of the research and statistical needs of the nation but whether this information can be made available to researchers in ways that protect confidentiality. Confidentiality bears on the accuracy and quality of the data in the network since without adequate protections, patients will be reluctant to be frank about facts which bear on their health.

In general, we believe that disclosures from this network of individually-identifiable information for the purpose of research should occur only when the individual has given consent for such a disclosure. It is important to note that this principle would not impede

the vast majority of statistical research, which explores patterns or relationships within populations, but almost never requires information that can identify particular individuals. Examples of this type of research include studies identifying high risk population groups, access to health care among vulnerable populations, and variations in the use of health care services or in outcomes of care.

While statistical analyses often require linked, person-level information (and unique identifiers are required to create such files), the researchers performing the analyses do not need to know the identification of the particular individuals from whom the information was obtained. Consequently, most statistical research needs can be met without compromising privacy through "public use" files that are stripped of all individual identifiers and any other information through which individuals could be identified indirectly. Both the Medicare program and the National Center for Health Statistics have excellent track records in creating such files and making them available to qualified researchers.

Some research, of course, does require access to individually-identifiable information. The creation of sampling frames to identify individuals for targeted surveys or for clinical or preventive trials is one example. Another is the linkage of encounter data to other information in longitudinal treatment or epidemiologic studies. In some studies, individuals can be given the option to participate voluntarily. In other cases, strict standards and careful review (including by Institutional Review Boards) are needed to ensure that no alternative to the use of individual identifiers is possible, that only the minimum amount of information necessary to carry out the study is released, and that stringent penalties are imposed for any misuse of data. All nonoperational uses of individually-identifiable data should be considered only in the context of carefully reviewed and approved research protocols.

One way to implement the legal protections for privacy of data used in research would be through the regional data centers. Regional data centers, which could be public or private and configured in a number of ways, could serve as research and statistical centers with some of the same legal protections as the Census Bureau. There would be a number of data centers, all of which could be immunized from the scope of reporting laws and judicial process, just as the Census Bureau is. The obligation to report diseases or to furnish records in a court proceeding would continue to apply to the individual provider, as is the case today. But we are considering shielding these new clusters of health information from that kind of access by the government, along the lines of the recommendation of the Institute of Medicine in its recent report, *Health Data in the Information Age.*

For their research and statistical functions, the regional data centers would link enrollment, encounter, and other data and perform the necessary work to remove individual identifiers before releasing data to researchers. Stringent penalties would apply to all persons who worked in the regional data centers and to all researchers who obtained data from them, to prohibit and punish anyone who improperly revealed individually-identifiable information

or who received public use files and then attempted to re-identify individuals in any manner.

As a final note, I would like to add that access to information in the network by other statistical agencies may be appropriate, such as access to enrollment data by the Census Bureau. In this instance, existing statutes and longstanding practices have successfully prevented invasions of privacy. Moreover, the benefits of these institutions securing access to data in the new system are overwhelming. Access by these agencies could either be determined appropriate by the National Health Board or could be clarified in the Act.

Let me conclude by putting the information aspects of the President's proposal in a broader perspective. The Health Security Act will reduce the burden and costs of recording health information while at the same time assuring that all participants have the information they need to carry out their functions and make informed decisions. This system will be surrounded by legal and operational confidentiality safeguards -- built into the design at the beginning and basic to its operation -- to protect the privacy of the people it serves. This combination of legal and other safeguards will offer the public assurance that individually-identifiable information will be used respectfully and carefully and will make it possible for all to benefit from the results of expanded research.

We look forward to working with you, Mr. Chairman, and other members of the Congress on these important issues.

Mr. SAWYER. Thank you very much for that very useful testimony.

When you talk about the kinds of protections that are afforded the Census Bureau, it really is protection from government itself that is, perhaps, the most important protection, from use for tax prosecution or other kinds of criminal prosecution, questions of national security, it simply is, not just a fire wall, but an absolute brick wall that stands between.

Would you see the same kinds of protection, with the exception of those that are—those access portals that spelled out otherwise, applying to this kind of data?

Ms. HUNTER. We do see the same kinds of protections in the sense that individually-identifiable medical information cannot be shared with another entity in such a way that the individual could be harmed along the lines of the examples you gave of prosecuting an individual or investigating an individual.

Mr. SAWYER. When it comes to the kinds of diseases that are, perhaps, most sensitive in our society, certainly AIDS and other problems of that kind, that really are the point at which you find public health interests and individual privacy coming in conflict with one another. How do you see that kind of conflict being resolved?

Ms. HUNTER. What we are discussing as an option is to immunize, as I said in my testimony, the Regional Data Centers from reporting laws. The state reporting laws and state public health laws would continue as they exist today, and they would continue to apply to providers who today have the obligations, which vary to some extent under state law, to report various diseases.

We would not alter the impact of those laws on individual providers.

Mr. SAWYER. You would keep that entirely separate?

Ms. HUNTER. We would keep that separate. What we are discussing is keeping that separate from the information in the Regional Data Centers.

Mr. SAWYER. And would there be any value in making those reporting requirements uniform, in order to make the protections uniform across the country?

Ms. HUNTER. Well, that would be, that goes beyond the scope of what we are discussing in terms of the Regional Data Centers.

Mr. SAWYER. Who ought to own a medical record?

Ms. HUNTER. Excuse me?

Mr. SAWYER. Who ought to own a medical record? Does the physician own it, or does the hospital own it, or do they own that portion of it that they contributed to that overall record? Does the patient own the record? Does the Central or Regional Data Center own the record?

Ms. HUNTER. I think that's a very complicated legal question. From the perspective of the privacy analysis, the issue is not necessarily one of ownership, because the individual patient acquires certain rights in the information, rights to prevent disclosure, rights to inspect the record, rights to correct the record. Those are all rights that are elaborated in the Health Security Act, and that has been the focus of our concerns with the privacy.

Mr. SAWYER. Who should be in control of the answers to those questions?

Ms. HUNTER. Well, the basic rules, if you will, in terms of privacy and confidentiality, would be established in a process of both legislation and regulation.

Mr. SAWYER. How long is it going to take to establish a system of the kind that you have contemplated in the legislation that's before us, or in the President's proposal, or any of the others? How long will it take to set it up? Not in global terms because I think clearly we all believe that well-established it will save us money rather than cost us money, but just simply in terms of start-up costs, how much will it cost to set it up and how long will it take?

Ms. HUNTER. Let me defer to one of my co-panelists on that question, if I might.

Dr. SILVA. Well, sir, Mr. Chairman, Mr. Petri, the Act lays out a series of milestones, much like in other bills. The first milestone is to define, in collaboration with major stakeholders in the industry, what are the standard forms for enrollment, eligibility and the financial transactions, and that's to occur one year after, or within a year from the enactment of the Act.

Approximately 270 days following that, plans and providers must use those forms, at least in paper, and preferably electronically, and a year following that the information—two years after the Act is established, the information system is up and running.

We certainly expect demonstration sites to occur within that two-year window. Our goal is to have the system operational within that time.

At the same time, within two years of the Act, the strong privacy protection legislation that Ms. Hunter described would be operational as well, so we see them moving parallel.

With respect to costs, there is a tremendous upswing in the private sector investment in health information, and we believe that because we have constructed this Act via strong public and private partnership, the federal role will be in technical assistance, which we've described, only rather than having to build the system. We don't see the federal government having to lay fiber cable, for instance, to make this happen.

Mr. SAWYER. I understand that. I mean, each of the pieces of legislation have timetables built into them. We built timetables into ours, and the information network component in the President's has a timetable built into it. I wouldn't want to be challenged to hold my breath beyond the endpoints, or even any of the mileposts in there. I'm really looking for a sense of the kind of range of time that it's going to take, and a sense of what we are going to have to do in terms of up-front investment in order to make the savings that we'd anticipate.

The truth is, that if we don't put something of this kind in place, then at least some of the proposals that are before the Congress simply can't go forward. It becomes the strangle point in the system, and without it we don't get the outcomes that are held out for this overall system.

So, I don't ask it as an idle question, and I don't mean to question the hoped-for timetables that are built into the legislation. I think those are important, but I'm trying to get a sense of range.

Dr. SILVA. Well, I think that from what we have seen as we've traveled around the country talking about the Act in our policy data collection phase, there are a number of institutions that are actually doing many of the features of the Act.

Our assessment is that two-year window is reasonable, because we are using today's technology. In fact, the real key linkage is to developing standards as rapidly as possible, which the industry has begged us to do.

Mr. SAWYER. Should one entity or divided entities be charged with responsibility for providing access on the one hand and ensuring privacy on the other? Should these be entities in tension with one another, who are competing toward a common goal, or should it be the same entity that makes decisions with regard to specific kinds of information, specific kinds of uses?

Ms. HUNTER. I think where we are focused right now is on further formulating the standards by which whatever entity performs that function operates, so that there will be clear and uniform standards, whether that entity is the board, whether that entity is Institutional Review Boards, that's an issue that we need to discuss further and we'd be happy to discuss with you further.

Mr. SAWYER. When you talk about Institutional Review Boards, and this will be my last question, do you envision individual research institutions, universities, institutes and various kinds of settings, making their own decisions about appropriate kinds of use of information, or would those be cleared through a more central adjudicatory process?

Ms. HUNTER. Well, I think that our concern and our desire is to look at the system that exists, and, of course, there is an existing system of IRBs.

Mr. SAWYER. Sure.

Ms. HUNTER. And, to develop a system that operates on uniform national standards, with allowing—not creating additional or unnecessary obstacles for researchers, while at the same time having in place sufficient controls on privacy and on review.

Mr. SAWYER. I guess in my mind, it comes down to this. I have great confidence in the responsible handling of information among those entities today for whom clear professional standards exist. I think, in large measure, those who handle information in that way do so within the bounds of almost religious fervor, in terms of their commitment to the integrity of the systems. It's just that they don't link up very well, and there are huge gaps among them.

My real concern is that the public, in some cases, believes that the information that exists today is far more secure than, in fact, it is. They are shocked when they see it violated in some way, and fear the kinds of things that we are trying to build as an even greater risk, rather than a lesser one. Trying to educate a public, both with regard to the risks that exist today, and the potential benefit that comes along, will be central to winning whatever confidence it's going to take to make this sort of thing come about.

Tom.

Mr. PETRI. I guess I just had a follow-up area I'd like to ask a question or two about.

Does it make any sense at all, or are there provisions that enable individual consumers, or patients, or whatever, to authorize the re-

lease of individual specific information? It sometimes may be of benefit to them, but it might be the kind of thing that they would be best able to determine. For example, you might have a chronic condition, where you require medicine every day, and you might like that information out because someone getting into that market could send you a letter saying, you know, why don't you buy it from me at 30 percent less, and it would be to your advantage, and it would help that market function, although the person already providing it might not like that very much. But, who is to decide that? The individual would seem to me to be the logical person. For example, AIDS, some people might not mind knowing—everyone knowing they are in the market for a cheaper AIDS specific. Other people would definitely not want that information out in the marketplace.

And so, I'm just thinking that—another example, not so sensitive, would be a wheel chair, if someone is in a wheel chair, everyone knows they are in a wheel chair, they might like that information, people being able to purchase a list and send them something about a better piece of equipment or whatever.

So, in a sense, disclosure might empower people or create better options or be to their economic advantage, and in our zeal to protect them in all circumstances, we might actually be hurting the people, you know, that we say we are trying to protect. Could you address that a little bit? Is that something we should be aware of, or is that—

Ms. HUNTER. Well, the Health Security Act does provide that disclosures of information can be made with the individual's consent. So, in any situation where an individual authorizes disclosure for a particular purpose, then upon the presentation of that authorization, then, as is today, as is standard in medical care situations, then that particular individual and that information would be disclosable.

So, the principle of individual consent is part of the system.

Mr. PETRI. So, it would be possible for some business, say, to be set up to send a disclosure form to everyone, once they have national health insurance, saying if you'd like information, this type of information disclosed or put in the market, check this box, then we'll make these lists available to commercial purchasers?

Ms. HUNTER. That's a different question, and that's a question that takes us to a different place, because there would be, presumably, standards for what constitutes informed consent, and what the disclosure would entail.

And, what we have focused on so far has been the issue of individual disclosure in the context of either medical care or research.

Mr. SAWYER. Let me just ask one final question. I would expect that we will be sharing other questions with you, and if you would be prepared to answer those in writing, it would be very helpful to us.

The bill that Dave Hobson and I have been using as the vehicle for these hearings has attracted some interest among other committees of major jurisdiction that are in the process now of assembling the elements of what may come before the full Congress later on next year.

Is there anything in that legislation that Dave and I have put together that gives you trouble? Are there areas where you think we ought to adapt what we have proposed? Are there voids in that legislation that need to be filled? If you can just talk about its weaknesses for a moment.

Ms. HUNTER. I'd like, if I could, to defer this question also to Doctor Lasker, one of my co-panelists.

Dr. LASKER. There are enormous similarities between the two bills, and I'd like to emphasize that first. And, I would be very optimistic that working together we could find something that we would all feel quite comfortable with.

I think the major differences right now relate to things, for example, your bill focuses mostly on federal health information, it's not targeted towards the reform system, and there are some differences. For example, in the representation on the decision-making bodies about standards, which are issues like that.

And, I think as we are thinking more about the privacy issues, and as you are, that may send us in certain directions in terms of functions of entities like Regional Data Centers, and you talk about value, added networks. We are using different terms for many of the same things.

But, we would be very happy to work together with you on the bills. I don't see any glaring differences that would prevent us from reaching a workable solution.

Mr. SAWYER. One final question.

We, on this subcommittee, have been looking at the Census, per se, as one of the fundamental cornerstones of the broader national statistical system, a system that has been decentralized in many ways, and that I think could lend itself to a very large-scale review, in terms of how we adapt that system that has come together piece by piece into a more useful whole.

It seems to me that the body of information that will arise from this health care system could begin to rival the Census itself as yet another baseline, another cornerstone from which to draw that larger system.

Are there elements that we need to be alert to as we attempt to craft this legislation with those larger goals in mind?

Ms. HUNTER. Well, as I indicated in my testimony, one of the things that we are again discussing and considering is the relationship in uses of enrollment data, not medical data, but enrollment data, that may come in—that will come into the new system, and the usefulness of that to the Census Bureau. The Census Bureau, as I indicated, is an example of an agency that has very, very stringent and successful privacy protections.

So, we are looking at that issue in our own discussions.

I would just ask Katherine if you wanted to comment further.

Ms. WALLMAN. Mr. Chairman, I think, the only additional comment that I would add to that is, as you are fully aware, we are all looking toward the year 2000 and beyond, particularly beyond, in some of the alternatives that we are talking about for basic enumeration of the population, and for making sure we deal with the differential undercount and similar problems.

Clearly, having this system on the horizon has been something that's attracted the attention of a number of people and something

that we'll be looking carefully into as part of the overall structure for future activities.

Mr. SAWYER. Thank you very much for your presence here today, and for your thoughtful testimony. It's very helpful.

Ms. HUNTER. Thank you, sir.

Mr. SAWYER. Our second panel this morning is made up of Doctor Marilyn Moon, a Senior Fellow at the Urban Institute, Doctor Roger J. Bulger, President and CEO of the Association of Academic Health Centers and the Chair of the Committee on Regional Health Data Networks, Institute of Medicine, National Academy of Sciences, and Doctor F. Thomas Juster of the Survey Research Center, Institute for Social Research at the University of Michigan.

We had hoped to be joined by Burt Singer this morning, who was unable to be with us.

Let me welcome you all. Feel free to summarize the text. Your entire written testimony will be included in the record, and you should feel free to focus and summarize as it suits your purpose best.

Doctor Moon.

STATEMENT OF MARILYN MOON, SENIOR FELLOW, THE URBAN INSTITUTE; ROGER J. BULGER, M.D., PRESIDENT AND CEO, ASSOCIATION OF ACADEMIC HEALTH CENTERS; AND F. THOMAS JUSTER, SURVEY RESEARCH CENTER, INSTITUTE FOR SOCIAL RESEARCH, UNIVERSITY OF MICHIGAN

Ms. MOON. Thank you. I appreciate the opportunity to be here today. I'm going to be brief, because I am also losing my voice this morning, as a result of the common cold. I hope some of the research that's going to come out of a national database might help us solve that problem.

My testimony speaks to the importance of a national database from the perspective of a researcher familiar with a very similar database, the administrative data from the Health Care Financing Administration. In many ways, we know a lot more about the elderly and the disabled in the United States than we know about the rest of the population because of the existence of that administrative data and the use to which it has been put. Experience with this data base offers examples of the creative uses to which it can be put and some of the limitations that it has, in terms of not offering as much information about individuals as we'd like. Also relevant is the lack of problems from that data. For example the government has achieved a successful protection of privacy, even though administrative records are made available to researchers even outside the government. To my knowledge, there has never been a real problem with privacy.

I would like to talk a bit about some examples of why a national health care data are so important. Analysis of quality in health care is going to be doubly important as we focus on the cost containment efforts.

In the past, we have tended to ignore both cost issues and quality. But now as we begin to ratchet down on spending on health care and try to limit the use of inappropriate services, we need to track the quality of care and to make sure that it does not suffer.

Although, a lot of quality research revolves around very detailed medical record information, the kinds of administrative and broad-based data that a national health system would allow, is also critically important. For example, we can look at what happens to mortality statistics over time on a broad population base. At present, we don't know, for example, once medical care is disseminated beyond very small controlled settings, what its impact is on the health of the population. A national database that extends beyond the elderly and disabled will allow us to track such mortality statistics.

Similarly, in terms of use of services, we now know from Medicare data how much variation there is across the United States on services for the elderly and disabled. For example, even between New Haven and Boston, two areas with excellent medical centers, there are unexplained and interesting differences in use of services (such as hysterectomies) that suggest the need for further study. Again, a broad-based ability to look at the rest of the population is important.

In the policy area where I do most of my work, improvements in data are also important for evaluating policy changes that may be put into effect. For example, if practice guidelines are instituted, what happens to the health care system? What's the response? Is it good? Is it bad? The responses to economic incentive changes will be critically important in tracking the success of the health care system reform, and we are going to need broad national data to do that.

Finally, data can help in understanding the prevalence of disease. Data would enable us to identify problem areas, for example, to look at clustering of cancer, or to look at clustering of contagious diseases.

Why are these data particularly unique in that respect? First of all, it's the size of the database. Obtaining a national database, a truly national snapshot of what's happening, as well as a look through time, are critical factors. Second, these would also be timely data, since they would be the same information used to pay providers. Some of the very high-quality data that we have now on health care is only available many years after the fact. For example, the National Medical Expenditure Survey, now being used for a lot of analysis was done in 1987, and the world has changed dramatically since then.

Third, reliability improves whenever you tie the data to the payment of bills. Collection of information improved dramatically from hospitals, for example, under the Medicare system when some changes were instituted that tied the information to how much hospitals would be paid. Reliability is enhanced with this kind of data system.

Expense is also reduced, because it's a byproduct of what we need to collect for other purposes.

Finally, it is also important to focus on issues of privacy and confidentiality. Here the relationship with other data is critical, that is the ability to link these data with other studies. It may be useful to be able to go back into the field, for example, and look at issues of why cancer is clustering in certain areas, or to look at adverse outcomes that we think we're seeing in certain areas. To track poor

practices of medicine, we need to be able to link records over time, and to go back to the same sources to get more detailed information.

I'm optimistic that protections for privacy can work well in this system. The HCFA database has a very good track record in this regard. Whenever you are dealing with a database of this sort, which is a large national database, it is relatively easy to protect privacy. Rather, the problems are more likely to occur at the original point of collection of the data. We enhance the problems by passing it on, for example, to regional and national levels.

Thus, while concerns about protecting privacy are important, I'm happy that this committee and others are now interested in trying to develops a national database and to make it available to reseachers. The database will be essential in understanding our health care system.

Thank you.

Mr. SAWYER. Thank you very much.

[The prepared statement of Ms. Moon follows:]

PREPARED STATEMENT OF MARILYN MOON, SENIOR FELLOW, THE URBAN INSTITUTE

I appreciate the opportunity to be here today to testify about the important contributions that a national data system on health care can offer and why such a system is an important element of reform. Much of the publicity surrounding the collection of data has focused on the negatives--problems of privacy and intrusion of government into our lives. But there is another side of the picture; although care needs to be taken regarding privacy issues, the benefits of developing a national data base far outweigh the costs. If we want to improve health care and better manage its delivery, it is critical to have reliable data.

My testimony makes three points:

- A national data system is important for achieving a number of goals: assuring quality, understanding how medical care is used in the United States, studying the impact of policy changes on health care, and studying the basic prevalence of health conditions across the country.

- Data collected as part of a national health care system would offer unique advantages for the types of research needed, and would represent the most efficient way to gather information.

- It is possible to safeguard privacy while making data available for medical and policy research.

While the issue of data collection is not central to many of the debates on health care reform, it is important to seize miss the opportunity to enhance our understanding of health care as part of any reform legislation.

The Importance of Data Collection Efforts

A national health data system could be a natural by-product of administrative information used to pay claims or track health care use within health care plans. It needs to be able to distinguish among plans, providers and patients, so that information could be gathered, for example, on how well plans are performing, what types of services doctors or hospitals are providing, and what range of services patients are receiving. More or less patient information might be appended to the data as well as other characteristics such as location of services. Since one of the goals of health care reform is a uniform reporting system to reduce administrative costs, data would be collected in a way that could provide consistent information across the country.

The closest analogy is with the Medicare administrative records collected by the Health Care Financing Administration. For covered Medicare services, data are collected on basic beneficiary characteristics including age, race, sex, reason for entitlement, dual enrollment in Medicaid, and residence. When claims are made for payment for Medicare covered services, additional data on types of services, charges for the services, diagnosis, dates of care, and provider identification numbers can then be added to a beneficiary's record.

These then allow the construction of, for example, a year's worth of care received by the beneficiary, or by provider, what services were billed. Even with the limitation that having only partial information offers, researchers have learned many things about this part of the population from these data. Many of the examples I use below are drawn from this data source.

In fact, we now know much more about use of services for Medicare beneficiaries than for the rest of the population because such data are not available for younger persons. Obviously, it is important to be able to do the types of analyses described below for the whole population since health problems and practices vary by group.

Quality Issues. One of the most important uses of any data base developed from reform should be analysis of the quality of health care received in the United States. Whatever reform might be adopted will likely emphasize controlling health care costs, and such efforts make oversight of quality even more important. The new incentives that reform sets up will likely encourage a leaner health care system and one which sometimes places limits on what services are covered or how care will be delivered. Vigilance over the quality of care thus becomes even more important as a check and balance on any reform.

Most of the reform proposals recognize the need for oversight of the system to protect its quality. For example, several of the reform proposals that have been introduced in the Congress suggest the need for health care ombudsmen to serve the role of patient advocates. Health care "report cards" are also often included. But these efforts require the careful collection and monitoring of data to inform that process. Some of this will take the form of patient satisfaction information, but other elements must include the monitoring of access to services and types of care delivered by plans in a given area. Moreover, it is important to share data across regions so that there is assurance of uniform national quality standards.

Data on outcomes of treatment are particularly important for quality studies. While very comprehensive outcomes studies require detailed analysis of patient records and other supplementary material, even basic administrative data can be informative. Patient mortality rates, hospital readmissions, and problems with hospital stays (such as infections or other incidents) are examples of data that can be gathered from administrative records. Medicare data have been used in this way to monitor the impact of hospital reforms, for example. Large scale studies, such as tracking mortality rates associated with specific procedures need such records. They allow researchers to look beyond the small number of carefully controlled cases that are studied while procedures are being introduced. We need to do much more to focus on how well procedures work in practice once they are fully diffused. Are procedures as successful once they are widely used as when originally analyzed in a controlled setting? Particularly if we are examining a relatively rare procedure, very large national data bases are needed.

Moreover, administrative records can serve as the starting point for identifying cases or situations that warrant further study. Sometimes linkages between the national data base

and patient records or other information will be needed. Research with Medicare data, for example, has been used to help analyze the appropriateness of certain procedures, leading to findings about unnecessary surgeries.

Use of Services. Interestingly, although we have a very sophisticated system of health care in the United States, it is often difficult to find good information on how many services of various types are performed and in what combinations. Health care use varies substantially across the United States, but those differences are not well understood in detail. What really are the norms of practice? Who is getting what types of care? These issues relate to both quality and cost considerations. They also speak to whether there are subtle biases in how different groups within the population are treated. Are women more or less likely to undergo certain procedures? What are the differences by race? Because we have administrative data for the elderly and disabled, researchers have begun to look at a number of these issues, but are limited to this part of the population.

For example, recent studies have focused on which ambulatory services are growing the fastest for Medicare patients. Research by some of my colleagues at the Urban Institute tells us about the diffusion of new technology in Medicare, which has both cost and quality implications. Other researchers have also noted enormous differences across various locations in the United States in the frequency of the use of operations, such as hysterectomies or prostatectomies. These studies have been used to suggest how the norms of care may vary across the country and they have been credited with changing the way that physicians practice medicine by calling attention to variations in treatment. Other studies have found that black Americans are much less likely to receive certain kinds of operations than are whites, even after controlling for possible differences in health status. These types of analyses require very large data bases to find enough cases of particular health problems to demonstrate national patterns. At present, we can only study the elderly and disabled in this way; no comparable data bases are available for the rest of the population.

Policy Studies. Health care reform proposals would often change the economic incentives or regulations affecting insurance plans and providers of health care in ways that are likely to influence how care is delivered in the United States. In order to assess the effectiveness of such changes and whether other, unintentional responses occur, it will be important to conduct research. Again, the type of data base that can be developed with reform is essential.

For example, in order to control costs we need to understand how health care resources are used in the U.S.: what areas are growing the fastest, what physicians or hospitals are operating outside the norms of accepted practice, how new technology is being used, and what patients are particularly heavy users of care. If there are multiple insurance plans, it is important to consider whether some seem to be more successful in holding down costs than others and why this is so. Data on use of services combined with charges can explain why spending varies around the country and whether some areas are more efficient in providing care or whether they are just low cost areas with low prices or low use of services.

Recent analysis of Medicare data, for instance, suggests that although Medicare is a national program, costs of providing care to beneficiaries vary in dramatic and puzzling ways across the country. The questions raised by this profiling suggest the need for more indepth analysis. Another example of policy-related research occurred around the introduction of Medicare hospital payment reform. These analyses have focused on questions such as what happened to mortality rates, hospital readmissions, and shifts in the sites of care to outpatient departments, home health and skilled nursing facilities. Both quality and cost containment questions were studied with administrative data.

Prevalence of Disease. In addition to all the other analyses described above, administrative data can be used to focus on specific diagnoses and determine whether there are, for example, concentrations of particular health problems that may indicate environmental or other factors. Pinpointing the residence of individuals with specific cancer diagnoses can tell us much about where to look for potential sources of hazard. Data on prevalence of communicable diseases would be of similar interest. The recent outbreak of a virulent type of flu in the Southwest, for example, was at first thought to be an isolated incident. Since then, we have begun to discover that its incidence is probably much more widespread. More timely availability of such information could have prevented some of the discrimination and unwarranted attribution of the problem to native Americans.

Why This Particular Type of Data?

Certainly the type of data being described here is not the only source of information on our health care system. We also rely on small controlled medical studies that analyze treatment, and on surveys such as the National Medical Expenditure Survey (NMES), the Health Interview Survey (HIS), or the Current Beneficiary Survey for Medicare (CBS). But these approaches complement and do not replace the need for use of a large national data base. The type of data system I am discussing here today offers a number of unique advantages, including the size of the data base, its timeliness, its reliability, its relatively low cost, and its importance to other data collection.

Size. For many of the studies described above, it is essential to have a very large data base. It not only needs to be national in scope, but it must capture enough cases to be able to look at rare diseases or treatments and to disaggregate the population into small groups by geography or population characteristics, for example.

Timeliness. Since data would need to be collected in order to pay bills, the information gathered will be very timely. Health care is changing rapidly in the United States and the older the data, the less valuable it becomes. For example, although the NMES offers an extremely rich data base, its most recent survey was conducted in 1987 and the data have only recently become available for public use. Many of the policy and even treatment issues that are relevant today cannot be effectively analyzed with seven-year old data.

Reliability. Since the data base we are discussing would be part of administrative files and linked to payment, they would have to be very reliable. Researchers have found, for example, that reporting of information such as diagnosis codes for hospital treatment improved markedly in reliability once they were required for purposes of compensation to the hospitals reporting the data.

Expense. As a by-product of other efforts, collection of these data would be relatively inexpensive. It is not economical to create a whole separate data collection outside the national health system. The size of the data base would have to be seriously compromised if this were the mechanism used.

Relationship with other data. Smaller, more detailed data bases can be dramatically enriched by linking with a national data base. For example, the CBS obtains detailed data on use of Medicare covered services from administrative records and supplements that with patient surveys. In this way, a reliable and less expensive data base is created. Moreover, studies that start with a national data base to identify problems, such as with quality of care, and then draw samples of patients or health providers to study further would also be invaluable. These uses make it essential to retain some patient and provider identifiers to allow linkages, subject to protections for privacy purposes.

Protections for Privacy

It is entirely appropriate to be concerned about privacy in developing the type of data base envisioned. But the problems of making sure that data flow into a national system create few additional risks, and with appropriate safeguards are well worth the effort. The problem of identifying patients and their medical histories arises as soon as anyone obtains the information. Leaks from physicians' offices or hospitals create a potential hazard, for example. The nature of a national data base, moreover, is that it is most useful to look at large quantities of data and individuals become much less important. Researchers do not need information that would specifically identify patients, so in most cases any identifiers could be stripped from the record or scrambled. Some centralized system to keep identifiers is needed so that records can be matched or linked in certain circumstances, but the numbers of persons with access to such information could be severely limited.

The use of administrative records for Medicare is a good case in point. These records contain patient and provider identifiers, but public use tapes for research purposes never include patient numbers. Moreover, although the government maintains these records, there has not, to my knowledge, ever been a problem of confidentiality surrounding this research.

Moreover, some of the uses to which leaking of confidential health data could be put will diminish after reform. Insurance companies would likely be forbidden to discriminate against patients, for example, so they will have less to gain from obtaining such information. Community rating of insurance would reduce employers' incentives to hire only healthy

workers. And if employers are less likely to self-insure, it would be harder for them to obtain information on their employees.

Conclusion

A national data system offers great promise for improving the health of Americans. Such a data base is essential for improving the quality of care and the efficiency of its delivery. It can help to identify misuse of resources and improve the quality of health care that people receive by identifying poor practices. It makes no policy or budget sense to obtain a national data base through other means. Privacy concerns should be an important part of the development of a national data base, but should not be used as a barrier to this important potential resource.

Mr. SAWYER. It just occurred to me when you were describing the importance and the uses of the kind of data that you were talking about, you realize what a thin film of ice we are standing on when you see the kind of thing that appears to be happening in Russia today, and how what may be perceived as relatively small changes in medical care and nutritional values can apparently alter the well-being of large segments of populations relatively quickly, quicker than any of us thought likely. There's a lot of data yet to be gathered, but it is a compelling phenomenon, at least as it appears from a distance.

Thank you very much for your testimony.

Doctor Juster.

Mr. JUSTER. Thank you, Mr. Chairman.

My written statement has two attachments. The first is a brief summary of the National Academy of Science's National Research Council panel report entitled, "Private Lives and Public Policy," and the second is a paper on confidentiality and privacy issues that was given some time back at the American Statistical Association.

Mr. SAWYER. Both will be included in the record.

Mr. JUSTER. Yes, they are in the record. Thank you.

I would like to address five specific issues. First, how important are the research uses of administrative record data, and how can these uses be enhanced without detracting from administrative uses?

Second, if administrative data are made available for research purposes, what types of protections against disclosure of sensitive information can be built into the process?

Third, how serious are the risks of disclosure—

Mr. SAWYER. Doctor, let me interrupt. I just realized I have a pending vote on right now. I've got three minutes to get over there. If you could just suspend for a couple of minutes, I'll go over, I'll be right back.

Mr. JUSTER. Sure.

[Recess.]

Mr. SAWYER. Doctor Juster, we were at point three, is that correct?

Mr. JUSTER. Yes, that is correct.

Just to briefly summarize points one and two so we don't lose them, the first point, how important are the research uses of these data, administrative record data? The second, if they are available, what types of protections need to be built into the process?

Third, how serious are the disclosure risks, and what procedures can be used to minimize those risks.

Four, what is the public perception of risk, regardless of what it actually is?

And, five, what restrictions should be placed on the use of such data for research purposes?

On the research potential, I think researchers with different disciplines will come to different judgments about this issue. My assessment is that the research value of administrative record data generally, including data relating to the health care system, is quite low when considered in isolation, but it is very substantial if the administrative data can be merged with other information.

The problem is that administrative record data of any sort, whether it be on earnings, medical treatment or health outcomes, health expenditures, disability benefits, cannot be used to understand behavior unless these data can be combined with other data, typically obtained from surveys, that measure a large number of characteristics for persons whose records are contained in the administrative database.

One way to see why this is so is to note that the administrative record data typically describe what I would call a set of very interesting outcomes, but contain no information with which these outcomes can be either explained or modeled.

Knowing the outcomes is important, but understanding why they take place is the essence of the research process, and understanding how behavior affects outcomes is of the essence for public policy research.

My guess is that my view of that would be different from someone who had a medical perspective, where I think the pure records are extremely valuable for that purpose, that's much less true for economic research, sociological research, social psychological.

It's useful to sort of turn the question around. How valuable are the data obtained from non-administrative sources, typically from surveys? Well, the answer is, of course, that while such data are extremely valuable, they often face a major limitation in the severe measurement error associated with the concepts that are either technically difficult, like a medical diagnosis, hard to recall, like historic earnings, or frequently not known by the respondent, medical expenditures covered by health insurance.

The optimum solution for research purposes is perfectly clear. Data are expensive to collect. Trying to find ways to share existing data with appropriate safeguards is in society's best interest. Thus, trying to find ways to combine the administrative records with other data obtained from surveys represents the best of both worlds, provided ways can be found to protect the privacy and confidentiality of the individual records.

What about disclosure risks? The general public, Congress, and the scientific community are legitimately concerned about the risks of disclosure of individually-identifiable data, whenever administrative record data are made available to others. What kind of protections can we put in place? Two sorts of things can be done, one administrative and one statistical. The administrative safeguards are to create a clean distinction between data collected or merged for research and statistical purposes and data collected for administrative purposes, and to erect and impenetrable wall between the two. The data collected that are merged for research purposes cannot be used for program administration or enforcement.

The National Academy Committee on Privacy and Confidentiality made precisely this kind of functional separation an important part of their recommendations, and it was one of the few recommendations on which the entire committee felt strongly and unanimously.

The argument is that the functional separation, where data collected for research and statistical purposes cannot be used for administration or enforcement, involves virtually no cost to society and considerable benefit. The only costs are that program administration or enforcement must generate its own administrative record

data, which is always essential anyway. But, functional separation means that data providers are assured that any information they give can be used only for statistical purposes, not for administrative decisions affecting specific individuals. In the absence of that assurance, data providers will soon come to realize that their agreement to participate in a research survey contains risks, and cooperation rates and data quality will predictably decline.

My own assessment of disclosure risk is that it basically depends on having a very detailed geography in addition to very detailed occupational characteristics. And, it's a fairly simple matter to limit both types of measures to relatively high degrees of aggregation, states or Census regions, something like two-digit codes on occupations.

I don't think it's true, incidentally, that disclosure risk is entirely a matter of stripping off identifiers. It depends on whether the person in a database has unique enough characteristics to where they can be identified by an outsider, and that's why geography is critical. If I know you live in Totowa Borough in New Jersey, I know a lot about you, and I can probably find you if I also know that you are a dentist. If I know that you live in New Jersey and that you are a professional with 20 years of schooling, I'm never going to find you. But, just those two pieces of data, dentist and Totowa, there are only six people like that in the world probably, so I can probably find you. So, that's where the risk comes from, it isn't just the identifiers, in terms of names and addresses and things of that sort.

Even though I think it's true that a realistic assessment is that disclosure risk, if properly handled, is small, that is clearly not what the public widely believes to be the case. I think the problem is that the public doesn't make a distinction between the use of information provided to public agencies for either research or administrative purposes, and use of information by private companies who are able to access databases relating to credit card uses, vehicle registrations and so forth.

Most people believe correctly that the identifiable information that they provide when they use their credit card will get to be known to mass marketers who will then use the information to develop a more efficient mailing list for their product. It is a reasonable inference, although it's wrong, that similarly identifiable information provided to the public sector, payments for health services, medical treatments, income tax filing, Social Security or disability applications and so forth, would also be available to anyone with enough ingenuity to look hard for it.

It is important, as I see it, for this committee to help with the public education process of explaining why it is that identifiable credit card data might well be available to anyone who wishes to buy the tape, but that identifiable earnings, medical treatments and other data are not available to anyone unless explicit authorization for that purpose is provided.

I think, Mr. Chairman, I'll close with just two comments, since I think you are probably running low on time. I'll skip the part I have about restrictions on use, in terms of general policies and informed consent. I'd just like to note that as a rule, as a policy, I'm in favor of requiring informed consent for access to administrative

data. I believe that there are justifiable exceptions to that, but I'd like to have them kind of—the presumption being that you need informed consent. To deviate, you need to justify your case to some kind of a data board.

I'd be much happier with that kind of arrangement.

Let me make two final points relating to policy issues. I made the argument that it's the merge of administrative databases and survey data which have the most potential for the kinds of research that I have in mind. Let me illustrate it with two problems.

Suppose you ask yourself, what is going to determine the future demand for long-term care facilities, and the future level of health expenditures in the U.S., in an environment in which we have a visibly aging population? Well, it's perfectly obvious that having administrative data on disease conditions and prognoses and expenditures is a critical part of being able to understand the consequences of various outcomes relating to disease. But, it's also true that there is a whole set of data relating to resources with which people can meet those long-term care needs. They can be met by going into a long-term care facility. They can also be met by having family support, from a spouse, from children, from siblings. It can also be met by hiring private care nurses, probably cheaper than a day care, than a long-term care facility. Your ability to do all that is a function of a lot of things about you as a person, which are not going to be in the administrative record base. You merge the two and you have a gold mine. That's the basic point that I'd like to leave with you.

Just let me illustrate with a second issue, not related to health care. Suppose you were concerned, as we are with what effects the changes in the Social Security laws are going to have, along with changes in pension characteristics on retirement decision, how long will people work, and on savings behavior. We have a national shortage of savings and an aging population. These are both critical macroeconomic issues.

It's perfectly obvious that you can't model these things without some estimate of people's lifetime income, because that critically determines what your savings rate will look like. In this society, lifetime income is a function of lifetime earnings, not just for the male person in the household, but for the female person in the household. You can't get those lifetime earnings other than from an administrative record file. You can't get them reliably.

What you want to do is to combine them, you want exposure to health risks, you want health care costs, you want a whole bunch of other information about the person, and about the household, you merge it with these earnings data and you have a major enhancement of your ability to do serious research which can yield both scientific insights and useful public policies.

Thank you.

Mr. SAWYER. Thank you very much.

[The prepared statement of Mr. Juster follows:]

PREPARED STATEMENT OF F. THOMAS JUSTER, SURVEY RESEARCH CENTER, INSTITUTE FOR SOCIAL RESEARCH, UNIVERSITY OF MICHIGAN

My name is F. Thomas Juster, and I am a Research Scientist and Professor of Economics at the University of Michigan. I am also a member of the National Academy of Sciences/National Research Council Panel on confidentiality issues relating to government statistics.

My comments will be directed to some points that are central to the issue of how systems of administrative records, including those relating to individual medical history or health expenditures, can be used to meet the needs of both health care policy makers as well as researchers. The general principles that I will discuss are quite broad, and apply to issues beyond those relating to health or medical records.

My testimony has two attachments. The first is a brief summary of the NAS/NRC Panel Report titled "Private Lives and Public Policy." The second is a paper on confidentiality and privacy issues that I gave a few years ago at a panel discussion on this topic at the Annual Meetings of the American Statistical Association.

I would like to address five specific issues:

1) First, how important are the research uses of administrative record data, and how can research uses be enhanced without detracting from administrative uses?

2) If administrative data are made available for research purposes, what types of protection against disclosure of sensitive information can be built into the process?

3) How serious are the risks of disclosure of administrative record data that are made available to the research community under specified conditions? And what procedures, both administrative and statistical, can be used to minimize disclosure risk?

4) What is the public perception of disclosure risk?

5) What restrictions should be placed on the use of administrative record data for research purposes?

1. The Research Potential of Administrative Record Data

Although other researchers might well come to different judgments, my assessment is that the research value of administrative record data, including data relating to the health care system, is very low when considered in isolation, but is very substantial if the administrative data can be merged with other information. The problem is that administrative record data of any sort-- whether it be on earnings, medical treatment or health outcomes, health expenditures, disability benefits, etc.--cannot be used to understand behavior unless these data can be combined with other data, typically obtained from surveys, that measure a large

number of characteristics for persons whose records are contained in the administrative data. Without knowing a good deal about the characteristics of individuals whose records are in the administrative system, it is not generally possible to understand what has caused the outcomes that are measured in the records. This it is difficult to use the data for scientific research, or for most public policy purposes. One way to see why this is so is to note that administrative record data typically describe a set of very interesting outcomes, but contain no information with which those outcomes can be either explained or modeled. Knowing the outcomes is important, but understanding why they take place is the essence of the research process, and understanding how behavior affects outcomes is of the essence for public policy research.

It is informative to turn the question around: how valuable for research purposes are the data obtained from non-administrative sources, typically from surveys? The answer is that while such data are extremely valuable they often face a major limitation in the severe measurement error associated with concepts that are technically difficult (medical diagnoses), are hard to recall (historic earnings), or are frequently not known by a respondent (medical expenditures covered by health insurance).

The optimum solution is perfectly clear, at least in principle. Data are expensive to collect, and trying to find ways to share existing data with appropriate safeguards is in society's best interests. Thus trying to find ways to combine administrative records with other data obtained from surveys represents the best of both worlds, provided ways can be found to protect the privacy and confidentiality of the individual records.

2. Protections Against Inadvertent Disclosure

Both the general public, Congress, and the scientific community are legitimately concerned about the risks of disclosure of individually identifiable data whenever administrative record data are made available to others.

There are a number of relatively straightforward steps that can be taken which will minimize, and in some cases come close to eliminating, disclosure risk. First, let me note that the main disclosure risk for administrative records probably rests within the federal government itself, rather than in the outside research or public policy community. Federal government statistics, particularly those collected for program administration or enforcement, necessarily contain a wealth of individually identifiable information; if those identifiers are also contained in other data records, then data from several sources can be merged--with or without informed consent.

What kind of protections can be put in place against unauthorized disclosure? Two sorts of things can be done, one administrative and one statistical. The administrative safeguards are to create a clean distinction between data collected (or merged) for research and statistical purposes and data collected for administrative purposes, and to erect an impenetrable wall

between the two so that data collected or merged for research purposes cannot be used for program administration or enforcement. (Whether the reverse should also be true is less clear.) The National Academy Committee on privacy and confidentiality made precisely this kind of functional separation an important part of their recommendations, and it was one of the few recommendations on which the entire committee felt strongly and unanimously. The argument is that functional separation, in which data collected for research and statistical purposes cannot be used for administration or enforcement purposes, involves virtually no cost to society and considerable benefit: the only costs are that program administration or enforcement must generate its own administrative record data, which is always essential anyway. But functional separation means that data providers are assured that any information they give will not be disclosed individually. In the absence of that assurance, data providers will soon come to realize that their agreement to participate in a research survey contains risks to them, and cooperation rates (and data quality) will predictably decline.

3. How Serious Are Disclosure Risks?

It is widely believed that data about individuals, even without explicit identifiability, are subject to serious disclosure risk, especially if a good deal of information is collected and if some of the information is longitudinal. The general idea is that knowing enough characteristics about participants in a survey will eventually enable a determined researcher to identify particular people, and no amount of statistical masking or aggregation can eliminate that threat provided there are enough different types of variables in the database.

That general notion is basically incorrect. My assessment of disclosure risk is that it basically depends on having very detailed geography in addition to very detailed occupational characteristics, and it is a fairly simple matter to limit both types of measures to relatively high degrees of aggregation--states or census regions on geography, something like 2-digit codes on occupation. And it is appropriate to have those detailed decisions reviewed by a data protection board whose members are sensitive to the disclosure risk issue. (There is an interesting illustration of how that might work based on my experience with merging Social Security earnings records with data from the Health and Retirement Survey, which I would be happy to discuss with the committee.)

4. Public Perception of Risk

Even though I would argue that a realistic assessment is that disclosure risk from the use of administrative data for research purposes is small, that is clearly not what the public widely perceives to be the case. I believe that the problem is that the public does not make a distinction between the use of information provided to public agencies for either research or administrative purposes and the use of information by private companies who are able to access databases relating to credit card uses, vehicle registrations, etc. Most people believe

(correctly) that the identifiable information that they provide when they use a credit card for a purchase will get to be known to mass marketers who then use the information to develop a more efficient mailing list for their product. It is a reasonable inference (although generally incorrect) that similarly identifiable information provided to the public sector--payments for health services, medical treatments, income tax filing, Social Security or Disability applications, etc., would also be available to anyone with enough ingenuity to look hard for it. It is important, in my view, for this committee to help with the public education process of explaining why it is that identifiable credit card data might well be available to anyone who wishes to buy the tape, but that identifiable earnings, medical treatments and other data are not available to anyone unless explicit authorization for that purpose is provided.

5. Restrictions on Use of Administrative Data

An important and controversial issue is: Should administrative data be available for research purposes without the explicit consent of the person whose data are in these records? A related issue is: Should explicit informed consent be required if people are in a database because they have applied for certain public benefits such as AFDC or Social Security? And a third issue is: What does informed consent really mean?

Reasonable people differ about whether or not informed consent is needed in order to permit the use of administrative record data for research purposes. It is clear enough that administrative databases obviously can be used for administrative purposes--that is why they were created. But should they be available to the research community without the explicit consent of the respondent? My own feeling is that informed consent should be required, that the data subjects should have the right to withhold use of their data for any purpose not directly associated with the program that created the database, and that the research process is not seriously impeded by an informed consent requirement that takes a reasonable view of what constitutes "informed" consent.

The cost of requiring informed consent is basically one of lower data quality--some respondents to a voluntary survey will not give consent, and they may behave differently from those who give consent, thus creating the possibility of statistical bias. But the cost is probably small if the informed consent request is carefully and accurately crafted. I have some personal experience there, again in conjunction with the Health and Retirement Survey, that I would be happy to share with the Committee, and I have included the informed consent statement used on that study. The appended summary of the NAS/NRC Panel (Private Lives and Public Policy) contains a thoughtful discussion of the issue.

Summary

I would make the following points:

1) Administrative record data, such as that proposed in the Health Care Information Modernization and Security Act of 1993, can make an invaluable contribution to scientific research and thus to public policy if it can be merged, given informed consent, with other data.

2) With reasonable care, the privacy and confidentiality of individually identifiable data can be safeguarded. Explicit legislation would also be very helpful.

3) Disclosure risks are much lower than is perceived by the public.

4) It is possible to work out informed consent procedures that are clear to survey respondents and that will have relatively high acceptance, although some loss of data quality is inevitable.

Attachments: HRS Permission Statement
Paper prepared for ASA Panel on Confidentiality
Excerpts from "Private Lives and Public Policy"

c:\heatherh\papers\testmony.316

Attachment to Testimony by Dr. F. Thomas Juster

Informed Consent Statement used on the Health and Retirement Study

The University of Michigan

INSTITUTE FOR SOCIAL RESEARCH / SURVEY RESEARCH CENTER – FIELD SECTION

426 Thompson Street • P.O. Box 1248 • Ann Arbor, MI 48106-1248

Health and Retirement Study
Permission Statement

To the Respondent:

We would like to obtain a history of your past earnings and any Social Security benefits you might have received. Since most people cannot recall this information very well, we are asking for your permission to obtain it from government records of:

1) Your past Social Security covered earnings and total taxable earnings, both of which appear on the W-2 forms that people get from their employers.

2) Any Social Security Benefits you may have collected.

The information we are requesting is protected by Federal law, and cannot be released to us without your written consent. The University of Michigan is committed to maintaining the privacy and confidentiality of all data obtained from or relating to our survey respondents.

If you give us your Social Security number along with your permission to collect this information from the Social Security Administration, we will combine it with the information you have provided in this interview.

We will remove your name, date of birth, and Social Security number, and release the resulting unidentified statistical information to interested researchers for research purposes only. Additional procedures will be adopted to ensure that you will not be identified as an individual in the survey.

To the Social Security Administration:

I authorize you to release to the University of Michigan, for use in the Health and Retirement Study, information on the amounts of any earnings in my Social Security records along with the industries in which I worked, and on the amount of benefits paid to me under programs administered by the Social Security Administration for the years 1937 through 1991. It is my understanding that the University of Michigan will protect the privacy and confidentiality of these data.

Social Security Number: ___ - ___ - ____

[PLEASE PRINT]

Full Name: _____
(First) (Middle) (Last)

Date of Birth: ____/____/____
(Month) (Day) (Year)

Maiden Name (if relevant): _____

_____ _____
(SIGNATURE) (DATE)

Attachment to Testimony by Dr. F. Thomas Juster

Paper from ASA Panel on Privacy and Confidentiality

ASA PANEL ON PRIVACY AND CONFIDENTIALITY DISCUSSION

F. Thomas Juster, University of Michigan
3240 ISR, P.O. Box 1248, Ann Arbor, MI 48106-1248

Introduction

My comments are addressed to a number of specific points. My major concern is an assessment of the benefits and costs from using administrative records data to enrich data collected of surveys, an area in which issues of informed consent, disclosure risks, masking procedures, and approval processes play major roles. The points that I want to address are:

1. What is the gain to society from facilitating linkages between administrative records and survey data?
2. What are the major disclosure risks if such linkages are permitted and/or encouraged?
3. Under which circumstances should survey records be available to administrative agencies, e.g., for enforcement of the Anti-trust laws?
4. What masking procedures make most sense from the perspective of the research uses of any combined administrative record and survey dataset?
5. What can be done to develop appropriate professional norms for minimizing disclosure risks?

Gains from Record Linkages

The primary gain from permitting or facilitating administrative record linkages with survey data is that it greatly enhances the scientific potential of the resulting databases. And to the extent that the quality of a database results in better scientific understanding, record linkages will not only help to improve the rate of scientific progress, but will improve public policy because it will provide a more solid knowledge base.

A good case in point would be the advantages to the Health and Retirement Study, now in the planning stages, of being able to add administrative data on earning obtained from Social Security files. In order to understand retirement decisions, analysts would be greatly aided by a reliable set of data on the earnings history of survey respondents. On the survey itself, we plan to include a fair amount of questions about earnings history, but because of space limitations and because respondents have limited ability to recall events in the more remote past, that history will be largely concentrated in the 10 years prior to the survey date.

Models of retirement decisions would like to use various measures of "human wealth"; for that purpose, reliable data on annual earnings over the respondent's lifetime is an essential ingredient. Rough approximations for the desired measure -- e.g., beginning and ending earnings on the respondent's current job, supplemented by occupation and education level -- are clearly much less satisfactory and could easily produce different estimates of the response of labor hours to financial variables like wage rates and pension incentives, to health conditions, to the pull of leisure activities and family responsibilities, etc. Moreover, as this longitudinal study proceeds and respondents become eligible for Medicare, one must certainly expect to get a better estimate of expenditures on medical care by accessing Medicare records than could possibly be obtained from survey questions asked of respondents. Thus the research uses (and to the extent that good science provides better public policy) and the policy uses of datasets like the HRS would be greatly benefited by combining administrative records with conventional survey measures.

Disclosure Risks

In any discussion of the risks associated with releasing microdata into the public domain, the point is often made that with sufficient information about the characteristics of a particular household, the risk of disclosure approaches virtual certainty. Thus the accumulation of longitudinal data for the same person or household, the measurement of a large number of characteristics of that person or household, and the combination of characteristics and administrative record data are often alleged to virtually guarantee that neither privacy nor confidentiality can be protected from a well-armed attacker bent on finding a specific person or household in a sample survey.

While I understand that computer matches, large numbers of characteristic variables, and large amounts of detailed financial data make it easier to imagine that a particular person or household could be identified from a public use file, it seems that most discussion fails to recognize the single most crucial distinction relating to disclosure risk -- does the determined attacker know whether a particular person is in the sample to begin with?

Let me make the point by illustration. If I know that a particular colleague of mine was in fact interviewed for the Current Population Survey, I have a pretty good shot at identifying that person. If from CPS (or SIPP)

files I can identify occupation, income, sex, race, age, and SMSA, I am quite likely to find that in the Ann Arbor SMSA there is only one CPS person with 20 years of schooling, an income between $50,000 and $75,000 annually, between 40 and 49 years of age, female, and with a professional occupation. If I know for sure that my female colleague was in the CPS sample, it is not difficult for me to imagine that I could find her. But if I have all that information but do not know whether that particular person is in the sample, then all I have discovered is that there is a female between the ages of 40 and 49 in the CPS who lives in the Ann Arbor SMSA, is a professional, and earns between $50,000 - $75,000 annually. There are probably between 200 - 2,000 people who fit that description, and I will have gotten nowhere in trying to identify this person on the basis of the information unless I know for sure that they are in the sample.

It is my judgment that this principle is quite pervasive. In short, if I know someone is in a particular micro database, I can almost certainly find them if you give me enough characteristics. If I don't know whether they are in the database, I can't find anybody unless the characteristics are such that there is only one such person in the entire area who fits a particular set of classifications. It is not difficult to see what types of disclosure risks might be faced, assuming you do not know that someone is in the sample. For example, geography and detailed occupation are clearly deadly -- if you tell me there is a dentist with income over $150,000 annually who has four children and who lives in Duluth, I can almost certainly find him or her. But if you tell me there is a professional person with that much income who has four children and lives in Minnesota, I am not going to get very far -- there must be several thousand people who fit that description. Thus knowing that I am looking for a rich dentist is enormously helpful if I am trying to find someone, and knowing that they live in Duluth is even more helpful.

The general principles seem to be pretty clear. The biggest risk factor is if someone tells me they are in a particular micro database that I have access to. If they tell me that, I am pretty sure I can find them. The next biggest risks are if someone tells me they are in a very specific occupation or in a specific geographic location -- how many Supreme Court judges or Senators are there who live in South Dakota? But if you give me one digit occupation codes and relatively gross geographic detail, I will have a good deal of trouble finding anyone regardless of how many characteristics the survey (or the combination of survey and administrative records) contains.

Statistical and Administrative Files

One of the important concerns relating to privacy and confidentiality is the degree to which datafiles designed for research and statistical purposes can be subverted to be used for enforcement purposes. The problem is illustrated with the recent case of EIA data obtained for statistical purposes being turned over to the Justice Department for use in an Anti-trust prosecution. Several points are worth noting about this issue.

The first and most important point is that a policy that permits the use of a research or statistical file (somehow defined) for administrative purposes must represent the worst cost-benefit ratio in recorded history. The benefit, in this case, consists of the change in the probability that offenders will be discovered and convicted, while the cost consists of future consequences in terms of survey response rates and data quality if respondents are told that the privacy and confidentiality of their data cannot be guaranteed if the records are subpoenaed by an enforcement agency. My assessment is that the benefits are vanishingly small and the costs are potentially enormous.

To see why the benefits are vanishingly small, ask yourself what could be learned that would be useful in an enforcement action that relates to the data content of any of the ongoing public or private surveys. Can I learn something from SIPP, or CPS, or the University of Michigan's PSID or SCF that would enable me to increase the odds that an offender would be caught and convicted? For household surveys, the question seems to answer itself -- there is nothing in the survey data that has the slightest prospect of adding to whatever information base any enforcement agency must already have: if I am suspected of tax evasion, it is hard to believe that whatever income numbers I gave to CPS would add credibility to the government's case that I had underreported my income. If they really had to depend on what I had told the CPS interviewer, the government is in bad shape indeed and someone's head should roll for incompetence. Whether a stronger case can be made for business surveys is not an area that I have any expertise in, but I have my doubts.

On the cost side, although it is far from clear that many respondents care about whether or not their data are held confidential, it is surely a loss if survey organizations (the Census or private organizations) cannot guarantee to respondents that their data will be confidential. The cumulative consequences for survey response rates and data quality, given a regime in which survey responses are routinely used for enforcement, would surely be large and would eventually destroy the usefulness of doing surveys at all. If for no other reason, ethics would require a survey interviewer to

begin by telling respondents: "Of course what you tell me must be turned over to the IRS or to the DEA, but I would certainly like you to answer these questions about your income and your drug use habits."

Masking Procedures

One of the important issues in safeguarding the privacy and confidentiality of survey responses is to ensure that data that are distinctive enough to have the potential for identifying a respondent are masked or blurred so as to prevent that from happening. Some blurring techniques are more damaging to the research uses of statistical data files than others. For example, a common method of masking is truncation -- all values above a certain limit are given the lower limit. It seems to me that truncation is one of the more damaging blurring techniques, and is substantially worse than some kind of averaging procedure, or what is worse yet, simply eliminating the potentially identifying characteristic. We have this problem with respect to the 1989 Survey of Consumer Finances, where there is a substantial sample derived from administrative files, with relatively high income and wealth. Truncation would make it impossible to talk meaningfully of changes over time in the distribution of income or wealth, while simple averages in groups of 5 or 10, starting from the top values, while it might distort some of the relationships, would clearly maintain the ability to do most analyses that researchers would be interested in.

Possibly the most difficult problem here is what level of geographic detail to incorporate in a public use file that has a good many other identifying characteristics of respondents. Geography is certainly one of the central variables when it comes to disclosure risks -- my comment above about the dentist in Duluth applies quite generally, and if the area is small enough and the person distinctive enough, identification will be possible if enough effort is put into it. For most research purposes, I would guess that even complete elimination of geographic detail would not make much difference. I know of very few analyses in which geography plays a crucial role. But that probably reflects my own research interests, and there are likely to be many researchers whose models would be significantly hampered by the absence of geographic detail. However, it ought to be possible to provide detail relating to size of place and nature of place, plus some geography that is large enough to eliminate distinctiveness, that should solve this problem. The main point here is simply that in our concern about minimizing disclosure risks, we should take care not to do unnecessary damage to the quality of the data.

Professional Norms

One set of safeguards that would help to minimize disclosure risks is to ensure that the community of academic users is fully apprised of the need to maintain the privacy and confidentiality of respondents in the microdata files that they are using. Hardly any researcher represents a threat here, since researchers typically have little interest in the idiosyncracies of microdata but are concerned with using the richness of microdata to estimate relationships in the population. However, there are many situations in which researchers inadvertently come to be aware of the identity of people in the files they are using, typically because masking or blurring was not considered when the files were put into the public domain. In at least one instance that I know of personally, that kind of problem arose on a study in which I came to know quite accidentally that two of the people in the sample were the (then) senior Senator from South Dakota and the (then) Governor of Alabama. Since my dataset had AFQT scores (the Army's version of the SAT), I could have published an IQ-like score for George McGovern and George Wallace! My understanding is that other researchers have quite inadvertently come across similar cases (how many black female judges are there in the state of South Carolina?). And I have seen other cases in which researchers interested in vignettes came close to publishing stories of hypothetical cases from the PSID file in which the PSID respondents would surely have been able to identify themselves from the story if they had happened to read it.

The best solution to this classic problem, which would also help in other problems, is to develop a set of strong professional norms, reinforced by penalties and/or licensing and/or bonding that provide unambiguous norms about appropriate safeguards and appropriate uses of statistical data.

There are several illustrations of the licensing/bonding process now in place -- PSID users, for example, have access to a data tape with much more refined geography if they enter into a licensing/bonding agreement than if they do not. And as a long term proposition, developing norms with penalties for deviant behavior seems like a highly desirable way to maximize the research potential of microdata while minimizing the risks to confidentiality and privacy.

Attachment to testimony by

F. Thomas Juster

before the

Subcommittee on Census, Statistics, and Postal Personnel

Committee on Post Office and Civil Service

U.S. House of Representatives

March 16, 1994

EXCERPTS

PRIVATE LIVES AND PUBLIC POLICIES

Confidentiality and Accessibility of Government Statistics

George T. Duncan, Thomas B. Jabine, and
Virginia A. de Wolf, editors

Panel on Confidentiality and Data Access

Committee on National Statistics
Commission on Behavioral and Social Sciences and Education
National Research Council

and the

Social Science Research Council

NATIONAL ACADEMY PRESS
Washington, D.C. 1993

The Panel's Charge and Areas of Major Concern

The Panel on Confidentiality and Data Access was charged by the Committee on National Statistics and the Social Science Research Council with developing recommendations that could aid federal statistical agencies in their stewardship of data for policy decisions and research. Three areas were of paramount concern in the panel's deliberations: protecting the interests of data subjects through procedures that ensure privacy and confidentiality, enhancing public confidence in the integrity of statistical and research data, and facilitating the responsible dissemination of data to users.

Legislation to Protect Confidentiality of Statistical Records

Recommendation 5.1 Statistical records across all federal agencies should be governed by a consistent set of statutes and regulations meeting standards for the maintenance of such records, including the following features of fair statistical information practices:

(a) a definition of statistical data that incorporates the principle of functional separation as defined by the Privacy Protection Study Commission,
(b) a guarantee of confidentiality for data,
(c) a requirement of informed consent or informed choice when participation in a survey is voluntary,
(d) a requirement of strict control on data dissemination,
(e) a requirement to follow careful rules on disclosure limitation,
(f) a provision that permits data sharing for statistical purposes under controlled conditions, and
(g) legal sanctions for those who violate confidentiality requirements (see Recommendation 5.3 for further discussion of this requirement).

Recommendation 5.2 Zero-risk requirements for disclosure of statistical records are, in practice, impossibly high standards. Regulations and policies under existing statutes should establish standards of reasonable care. New statutes should recognize that almost all uses of information entail some risk of disclosure and should allow release of information for legitimate statistical purposes that entail a reasonably low risk of disclosure of individually identifiable data.

Recommendation 5.3 There should be legal sanctions for all users, both external users and agency employees, who violate requirements to maintain the confidentiality of data.

Recommendation 3.1 Federal statistical agencies should follow a flexible, multilayered approach to informing data providers of the conditions under which they are being asked to provide information.

Basic information should be given to all data providers. Those who want more information should have the opportunity to obtain it directly from interviewers or by other means, such as supplementary written statements or toll-free telephone inquiries to the agency. The goal should be to give each data provider as much information as is necessary to make his or her consent as informed as he or she wishes it to be.

Recommendation 3.2 Basic information given to all data providers requested to participate in statistical surveys and censuses should include

(a) for data on persons, information needed to meet all Privacy Act requirements. Similar information is recommended for data on organizations, except that the requirement to inform providers about routine uses (as defined by the Privacy Act) is not applicable.

(b) a clear statement of the expected burden on the data providers, including the expected time required to provide the data (a requirement of the Office of Management and Budget) and, if applicable, the nature of sensitive topics included in the survey and plans for possible follow-up interviews of some or all respondents.

(c) no false or misleading statements. For example, a statement that implies zero risk of disclosure is seldom, if ever, appropriate.

(d) information about any planned or potential *nonstatistical* uses of the information to be provided. There should be a clear statement of the level of confidentiality protection that can be legally ensured.

(e) information about any planned or anticipated record linkages for statistical or research purposes. For persons, this notification will usually occur in conjunction with a request for the data subject's Social Security number.

(f) a statement to cover the possibility of unanticipated future uses of the data for statistical or research purposes.

(g) information about the length of time for which the information will be retained in identifiable form.

To meet the requirements of item (b), agencies must determine which of the data they plan to collect may be considered sensitive by data providers. As the authors of Statistical Policy Working Paper 2 concluded, there are no general rules for establishing whether data are sensitive. That decision involves community standards and generally must be made on a case-by-case basis. However, financial data—like income and assets—and data on illegal or ethically questionable behavior are typically understood to be sensitive.

In preparing an informed consent or notification statement, a statistical agency should carefully review the purposes and design of the data collection activity, especially when multiple contacts with respondents or linkages with data from other sources are planned or may prove to be desirable. Agencies should seek expert opinions as to what kinds of data are currently or may in the future be relevant to the goals of the statistical or research activity. Even experts, however, cannot foresee all future needs. Item (f) is intended to allow for unanticipated statistical and research uses of the data that are not inconsistent with provisions of the initial statements to data providers.

With regard to item (g), some statistical records, such as those from the decennial censuses of population, may be retained permanently in identifiable form. The subject of archiving of statistical records is covered in Chapter 6.

In general, similar information about statistical uses should be given to persons or organizations that are asked to provide information about themselves for compliance or programmatic (administrative) purposes, whenever there is a possibility that their data will also be used for statistical purposes. In such instances, it is likely that the major concern of data providers will be with the nonstatistical uses of their data, so that the basic notification statement should emphasize that aspect, rather than statistical uses. However, full information on statistical uses should be available to data providers who want it.

Data Sharing Within Government

A substantial amount of data sharing occurs between agencies for statistical and research purposes. Nevertheless, some of the laws that govern the confidentiality of statistical data prohibit or severely limit interagency sharing of data collected by some agencies. Laws that control access to administrative records, such as tax returns and earnings records, restrict their use for important statistical applications. As noted by the Council of Economic Advisers (1991), barriers to data sharing for statistical purposes have led to costly duplication of effort, inconsistencies among related data sets, and excessive burden on individuals and organizations who are asked to supply information. They have also made it difficult or impossible to develop data sets needed for policy analysis on important topics, such as trends in income distribution and the long-range consequences of occupational and other environmental exposures to suspected carcinogens.

> **Recommendation 4.1** Greater opportunities should be available for sharing of explicitly or potentially identifiable personal data among federal agencies for statistical and research purposes, provided the confidentiality of the records can be properly protected and the data cannot be used to make determinations about individual data subjects. Greater access should be permitted to key statistical and administrative data sets for the development of sampling frames and other statistical uses. Additional data sharing should only be undertaken in those instances in which the procedures for collecting the data comply with the panel's recommendations for informed consent or notification (see Recommendations 3.2 and 3.3).

The panel supports the proposal of the Council of Economic Advisers (1991:6) that legislation be developed that would permit "limited sharing of confidential statistical information solely for statistical purposes between statistical agencies under stringent safeguards."

Proposal for an Independent Advisory Board

Unlike other advanced industrial societies, the United States does not have an independent advisory board or commission charged with promoting effective implementation of the Privacy Act and other information legislation. There have been recent proposals by privacy advocates and legislators to create such a body.

Recommendation 8.5 The panel supports the general concept of 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. Any such advisory body should promote the principle of functional separation and have professional staff with expertise in privacy protection, computer data bases, official statistics, and research uses of federal data.

The experience of other countries has shown that data protection agencies can be a source of additional oversight for statisticians and researchers, subjecting their activities to greater scrutiny, promoting balance in data protection and data dissemination, and generating public debate. In some instances, new restrictions have been imposed on practices that do not appear to pose a threat to the confidentiality of individual data. Nevertheless, the panel believes that creating a positive climate for enhanced data protection and data dissemination requires assurances from many different quarters that legitimate protective policies and procedures are in place and are being followed.

An independent advisory board, with appropriate professional staffing, could constitute a regular source of expertise on a wide spectrum of privacy issues, including those related to research and statistics. It could give advice, serve as a sounding board for data protectors and data users, and offer legitimacy to responsible initiatives by both groups. The advisory board could provide support for responsible access to personal data as needed to realize the fundamental goals of democratic accountability and constitutional empowerment, which we introduced in Chapter 1. A professionally competent, respected advisory body could also act as a mediator when there are differences of opinion among data providers, privacy advocates, data users, and statistical agencies. Orderly evaluation and resolution of such differences by an impartial ombudsman could reduce the likelihood of their escalating to the point at which they seriously disrupt key data collection and dissemination activities.

Data protectors can and should be important allies of official statisticians and the general public in the achievement of an appropriate balance between the privacy interests of individuals and societal needs for research and statistical data about a complex society. In particular, data protectors can help statistical agencies resolve difficult issues in the areas of informed consent, confidentiality, data access, and record linkage.

An advisory body could also promote harmonization of disparate interpretations of federal regulations under the Privacy Act of 1974 or other legislation covering all or part of the federal statistical system. It could disseminate information about innovative techniques to permit the exchange of data for statistical uses without diminishing the protection offered to individuals, and it could provide oversight of agency practices in maintaining and disseminating sensitive information.

Mr. SAWYER. Doctor Bulger?

Dr. BULGER. Thank you, Mr. Chairman.

I believe I've been asked here because over the past two years I've served as the Chair of the Institute of Medicine's Committee on Regional Databases, which has the title, "Health Data in the Information Age: Use, Disclosure, and Privacy."

Mr. SAWYER. That, plus the fact that you are a good person.

Dr. BULGER. I see. Well, thank you for that compliment but I know you don't know that for sure, right?

By not talking about privacy and security today, I don't mean to minimize these issues. I merely think that they have been discussed already at length. What I'd like to do is to emphasize a couple of the uses of health data, to put these uses in terms that may be slightly different from some of the others that we've heard today so far, and to do that very briefly.

To illustrate my message, I have brought with me a group of articles that I took this week from two of the country's leading medical journals. One is a position paper, "The Oversight of Medical Care: A Proposal for Reform," from the American College of Physicians which says, in part, "Evidence suggests that the principal process of review, the case-by-case review of medical care, may not be cost effective and may not be conducive to improving quality. It should be replaced by profiles of practice patterns at institutional, regional or national levels." In other words, this article recommends that we tap into data that have been aggregated, abstracted and electronically transmitted, and that are sitting in a regional database, or perhaps even now in a Medicare database at the national level.

The New England Journal of Medicine has a special article on physician profiling—the same general issue—entitled, "An analysis of in-patient practice patterns in Florida and Oregon." The authors identify two different characteristics of physician behavior in these two states, and claim that by examining these characteristics in detail, and, in some cases, going back into the records, they were offered an opportunity to understand the differences and to improve patient care.

Now, my point in bringing this up, as someone recently did in an editorial about the use and abuse of practice profiles, is to note that looking into records that are three years old is not very meaningful if you are trying to improve practice right now. But what we are looking at in terms of the technology now in our hands is the capacity to really analyze what's going on in almost real time, and that's the vision and the prospect.

The second point made in these articles is that we don't know what's going to come up as people explore ways in which to use these kinds of data to all our benefits.

I would also like to point out the studies of appropriateness that Bob Brook and others have done using Medicare data. They were able to take diagnosis X, then go to the Institutional Review Board and say that they wanted to study diagnosis X and various treatments, or a particular treatment, and whether or not it was used, and if so, whether or not it was used appropriately. They wanted to look across several parts of the country and compare data.

Because there was patient identifiable data, they were able to examine specific records and drew some conclusions about the rate of appropriate care in different states and different regions of the United States.

They did not get informed consent from each of the patients whose record was examined, though it was understood that once you come into this environment that your record may be examined for the purpose of making comparisons. These studies are very important; similar studies are being conducted all the time.

Outcome studies are now being discussed more frequently. In outcome studies, you do the same sort of thing: go back and check with patients a year later and ask, did this operation really help you? The doctor says it was a success, but did it change your life? How did it change your life? Did you go back to work or not? With these kinds of studies we'll have a chance to really assess more accurately how useful particular interventions are.

Well, there is a genetic revolution going on right now. Paradoxically, we are in the midst of probably the greatest proliferation of new kinds of interventions in the health field that we have ever had. The science has been building continuously, and the new technologies are here, and they are not cheap.

New technologies may, in the end, save some money, and enable us to learn that we get better value if we use an intervention than we do if we don't. But we are here in a setting where we are trying to save money, or at least reduce the cost escalation, and what we are confronted with is a dazzling array of new approaches. I think it is possible that if we do not have the most spectacular and efficient information system, that we maximally utilize, we are simply not going to be able to manage all of the things we'd like to get out of our health care reform efforts. The proliferation is very intense that it costs many thousands of dollars to treat Gauchet's disease, which is a very rare disorder raises the question of balancing allocations of our resources between treatment for a few and prevention for many.

I think that policymakers and people judging how to expend money for health care are going to need health outcomes data, and I'm delighted that you are taking the time and interest to consider this issue.

Thank you very much.

Mr. SAWYER. Thank you.

[The prepared statement of Dr. Bulger follows:]

PREPARED STATEMENT OF ROGER J. BULGER, M.D., PRESIDENT AND CEO, ASSOCIATION OF ACADEMIC HEALTH CENTERS

Mr. Chairman and members of the subcommittee, I am Roger J. Bulger, M.D., President of the Association of Academic Health Centers. I have been asked here because over the past two years I have served as chairperson of the Institute of Medicine Committee on Regional Data Bases which recently issued its report entitled, "Health Data in the Information Age: Use, Disclosure, and Privacy."*

I wish to congratulate the subcommittee on these hearings; as a citizen, it is tremendously reassuring to realize the intensity and quality of your interest in these matters. I am aware of the previous testimony you have taken and have read the detailed discussions of privacy, confidentiality and security in the testimony of others. The IOM committee report delves significantly into these issues and expresses itself on the need for federal pre-emptive legislation to protect privacy, the development of a "fairness doctrine" concerning the public release of data identifying specific health care providers and the need for administrative rules and behaviors at the organizational level designed to make person-identifiable data more secure. I will in these comments today focus on the benefits and potential benefits of the collection and wise use of large data sets in the health care environment.

At the moment the following assertions may serve to describe the situation:

1. There is the capacity for developing regional data bases--electronically transmitted data abstracted from the patients record--for patient encounter data, for cost and financial data, and for billing purposes.

   Insurance companies have such data stored centrally which can be searched to decide issues related to issuance of life insurance or to determine whether for a given claimant patient there is a record of pre-existing illness not otherwise declared.

2. Other data sets, such as Medicare maintains, can be used to carry on useful clinical evaluative studies such as Brook's appropriateness investigations, which indicated that 14-42 percent of various procedures were inappropriate.

3. New York state has used such data as the basis for evaluative research allowing for comparisons of outcomes of cardiac surgery.

*See attached for the IOM Committee's recommendations.

4. In Pennsylvania recently, similar studies seemed to demonstrate that in some hospitals, effective care is rendered for one-third of the price compared with other institutions.

5. Regional data base organizations could collect, collate and disseminate such information with greater speed.

6. The Institute of Medicine study explores the benefits and risks of the development of Health Data Organizations (HDOs), whose function it would be to effectively collect and distribute data in appropriate form to the public. In addition to recommending the establishment of such regionally-based HDOs, the study also delineated the legal and behavioral boundaries of such entities and described necessary legal and administrative safeguards to protect privacy and confidentiality. The committee carefully delineated the short list of people who would be granted access to person identifiable information, but clearly recommended that provider identifiable data be provided.

   If managed care is to provide the opportunity for informed consumer choice among competing health care systems, it will be crucial for there to be a data base adequate to the task. The data base organization must have access to the expertise necessary to ensure the collection of worthwhile data which can be converted easily into a format allowing comparison with similar data in other regions. All of this is doable now.

   The Computer Patient Record (CPR) is waiting in the background for the opportunity to enter full time, universal service. The CPR can be in every doctor's office and would be the heart of his/her work station. The electronic patient record and work station offers the following advantages:

   a. the doctor can interact over diagnostic and therapeutic decision making;
   b. realtime epidemiologic data can be collected;
   c. clinical protocols can be effectively implemented;
   d. communication with referring doctors and medical libraries is quickly available; and
   e. population-based health status information can be updated instantaneously.

This electronic information highway, therefore, offers us unprecedented benefits.

In closing let me relate the implications of the benefits of properly organized electronically-transmitted data systems to the major concerns of health care reform. Our society seeks the best value for its health care dollar which means being able to choose the most effective and economical diagnostic and therapeutic approaches. We are well into an era of phenomenal proliferation of scientific and technologic advances; we are only at the beginning of the genetic revolution and face a cornucopia of expensive and

effective interventions at a time when we must seek with due diligence to control our rate of increase in spending. When we add to this agenda the goal of providing financial access to care for those currently unfunded, the need is apparent for the capacity to have rapid and ongoing evaluation to minimize wasted or inappropriate efforts. It can be argued that only the dramatic intervention of a superb information system can help us meet the objectives of health care reform.

Health Data in the Information Age: Use, Disclosure, and Privacy

Molla S. Donaldson and Kathleen N. Lohr, *Editors*

Committee on Regional Health Data Networks

Division of Health Care Services

INSTITUTE OF MEDICINE

NATIONAL ACADEMY PRESS

Washington, D.C. 1994

THE FUTURE

Little is yet known about how HDOs will function, what will be their likely benefits, or how they will evolve over time. In emphasizing the use of aggregated health information, the Clinton Administration's health reform proposal has put the issue of confidentiality squarely on the agenda. What is not known is which uses of health care information will be acceptable and will wisely serve the needs of society. Moreover, new uses for and users of data will emerge, some raising new threats to privacy. Accordingly, the privacy dimension of health care information is dynamic and should be revisited from time to time.

Regional HDOs hold tremendous promise for evaluating and improving health care and implementing effective new ways to protect health information. Although the great public benefit may be easily understood, the potential for harm or lack of fairness may create concern and fear in many. To gain public support for the vision advanced in this report--and to ensure the best public use of the health-related information that will be released--HDOs, government agencies, and public- and private-sector institutions must implement carefully planned strategies for fairness and privacy protection and educate the public, health care providers, policymakers, and patients about these protections. This report is intended to be an early step in that educational and public policy-making process.

BOX S-1 COMMITTEE RECOMMENDATIONS

RECOMMENDATION 2.1 ACCURACY AND COMPLETENESS

To address these issues, the committee recommends that health database organizations take responsibility for assuring data quality on an ongoing basis and, in particular, take affirmative steps to ensure: (1) the completeness and accuracy of the data in the databases for which they are responsible and (2) the validity of data for analytic purposes for which they are used.

Part 2 of this recommendation applies to analyses that HDOs conduct. They cannot, of course, police the validity of data when used by others for purposes over which the HDOs have no a priori control.

RECOMMENDATION 2.2 COMPUTER-BASED PATIENT RECORD

Accordingly, the committee recommends that health database organizations support and contribute to regional and national efforts to create computer-based patient records.

RECOMMENDATION 3.1 CONDUCTING PROVIDER-SPECIFIC EVALUATIONS

The committee recommends that health database organizations produce and make publicly available appropriate and timely summaries, analyses, and multivariate analyses of all or pertinent parts of their databases. More specifically, the committee recommends that health database organizations regularly produce and publish results of provider-specific evaluations of costs, quality, and effectiveness of care.

RECOMMENDATION 3.2 DESCRIBING ANALYTIC METHODS

The committee recommends that a health database organization report the following for any analysis it releases publicly:

- general methods for ensuring completeness and accuracy of their data;
- a description of the contents and the completeness of all data files and of the variables in each file used in the analyses;
- information documenting any study of the accuracy of variables used in the analyses.

RECOMMENDATION 3.3 MINIMIZING POTENTIAL HARM

The committee recommends that, to enhance the fairness and minimize the risk of unintended harm from the publication of evaluative studies that identify individual providers, each HDO should adhere to two principles as a standard procedure prior to publication: (1) to make available to and upon request supply to institutions, practitioners, or providers identified in an analysis all data required to perform an independent analysis, and to do so with reasonable time for such analysis prior to public release of the HDO results; and (2) to accompany publication of its own analyses with notice of the existence and availability of responsible challenges to, alternate analyses of, or explanation of the findings.

RECOMMENDATION 3.4 ADVOCACY OF DATA RELEASE: PROMOTING WIDE APPLICATIONS OF HEALTH-RELATED DATA

To foster the presumed benefits of widespread applications of HDO data, the committee recommends that health database organizations should release non-person-identifiable data upon request to other entities once those data are in analyzable form. This policy should include release to any organization that meets the following criteria:

- It has a public mission statement indicating that promoting public health or the release of information to the public is a major goal.

Continued

- It enforces explicit policies regarding protection of the confidentiality and integrity of data.
- It agrees not to publish, redisclose, or transfer the raw data to any other individual or organization.
- It agrees to disclose analyses in a public forum or publication.

The committee also recommends, as a related matter, that health database organizations make public their own policies governing the release of data.

RECOMMENDATION 4.1

The committee recommends that the U.S. Congress move to enact preemptive legislation that will:

- establish a uniform requirement for the assurance of confidentiality and protection of privacy rights for person-identifiable health data and specify a Code of Fair Health Information Practices that ensures a proper balance among required disclosures, use of data, and patient privacy;
- impose penalties for violations of the act, including civil damages, equitable remedies, and attorney's fees where appropriate;
- provide for enforcement by the government and permit private aggrieved parties to sue;
- establish that compliance with the act's requirements would be a defense to legal actions based on charges of improper disclosure; and
- exempt health database organizations from public health reporting laws and compulsory process with respect to person-identifiable health data except for compulsory process initiated by record subjects.

RECOMMENDATION 4.2

The committee recommends that health database organizations establish a responsible administrative unit or board to promulgate and implement information policies concerning the acquisition and dissemination of information and establish whatever administrative mechanism is required to implement these policies. Such an administrative unit or board should:

- promulgate and implement policies concerning data protection and analyses based on such data;
- develop and implement policies that protect the confidentiality of all person-identifiable information, consistent with other policies of the organization and relevant state and federal law;
- develop and disseminate educational materials for the general public that will describe in understandable terms the analyses and their interpretation of the rights and responsibilities of individuals and the protections accorded their data by the organization;
- develop and implement security practices in the manual and automated data processing and storage systems of the organization; and
- develop and implement a comprehensive employee training program that includes instruction concerning the protection of person-identifiable data.

RECOMMENDATION 4.3

The committee recognizes that there must be release of patient-identified data related to the processing of health insurance claims. The committee recommends, however, that a health database organization *not* release person-identifiable information in any other circumstances *except* the following:

- to other HDOs whose missions are compatible with and whose confidentiality and security protections are at least as stringent as their own;
- to individuals for information about themselves;
- to parents for information about a minor child except when such release is prohibited by law;
- to legal representatives of incompetent patients for information about the patient;
- to researchers with approval from their institution's properly constituted Institutional Review Board;
- to licensed practitioners with a need to know when treating patients in life-threatening situations who are unable to consent at the time care is rendered; and
- to licensed practitioners when treating patients in all other (non-life-threatening) situations, *but only with the informed consent of the patient.*

Otherwise, the committee recommends that health database organizations not authorize access to, or release of, information on individuals with or without informed consent.

RECOMMENDATION 4.4. RESTRICTING EMPLOYER ACCESS

The committee recommends that employers not be permitted to require receipt of an individual's data from a health database organization as a condition of employment or for the receipt of benefits.

PREPUBLICATION COPY
UNCORRECTED PROOFS

Health Data in the Information Age: Use, Disclosure, and Privacy

Molla S. Donaldson and Kathleen N. Lohr, *Editors*

Committee on Regional Health Data Networks

Division of Health Care Services

INSTITUTE OF MEDICINE

NATIONAL ACADEMY PRESS

Washington, D.C. 1994

The full report and separately bound summaries will be published and available from the National Academy Press in early March, 1994. To order, please call 1-800-624-6242 or 202-334-3313. For further information about the report, please call 202-334-2165.

Preface

From the very first meetings, in the early 1970s, of the newly constituted Institute of Medicine (IOM) of the National Academy of Sciences, a major objective has been the engagement of the most important and difficult health and science policy issues from the public's or society's perspective. The Institute was created so that a broad-based and multidisciplinary membership could work across professions, within and without the health sciences, toward the solution of these complex and difficult problems.

From my personal experience as a staff member at the IOM during the first four years of its life, I can attest to the early recognition of the importance of the process of having a balanced, multidisciplinary committee working on the policy issues at hand. The assumption was that the sum of the parts of such a diverse group was surpassed by the synergy of the whole; more often than not, this positive learning experience also produced a useful document or report. In my personal experience with such groups, I cannot recall a failure either in the product and its value or in the process and its impact on the individuals participating. I must say, however, that the challenges facing this committee on regional databases were so great and our initial difficulties so intense in becoming clear about and comfortable with the seminal questions embedded in our charge that I was not optimistic about either our two-year experience together or the product that I could envision emerging.

Our challenges were formidable because the very nature of the "regional databases" was obscure to some, their potentials for good or harm were obscure to others, and the interweaving of such heavy strands of legal material with information technology, data management, security maintenance, and the substance of health services research made it exceedingly hard for many of us to get comfortable with our view and understanding of the completed policy tapestry.

But we did it! Never have I been on a committee with the dogged determination of this one; our relatively large committee seldom had a meeting wherein even one, let alone more than one, member was absent, and they stayed to the end. Never have I been on a committee wherein the doctors, scientists, data experts, lawyers, representatives of the public interest, and experts from the business world had such great expertise, such strong opinions, and such diverse perspectives.

The key to the success of this project, it seems to me, was the gradual emergence of a commonality in shared values. Somewhat to our collective surprise, we found ourselves unanimous in our acceptance of the following fundamental assumptions: (1) use of population-wide databases developed from individually collected, computerized personal health data has become a working reality; (2) potential benefits of such data sets used for financial, organizational, quality improvement, and research purposes to society are indeed great; (3) protection of the individual record from person-identifiable exposure must involve all possible behavioral, systematic, and technical security measures; (4) relevant data sets and analyses including hospital-, clinic-, and provider-specific data must be expeditiously made available to the public; and (5) bona fide researchers must have access to person-identifiable records in order to provide society with timely studies on health status and health care.

These five foundational elements were essential to the committee's collective thinking and its observations, conclusions, and recommendations as detailed in the report.

Once the committee came together around these ideas, it was able to move systematically through the myriad of policy implications that come from reasoning from basic principles. This could not have been accomplished without the indomitable persistence and prodigious intellectual work of Molla

Donaldson and Kathleen Lohr. Karl Yordy made key contributions intermittently as was appropriate for an IOM division head.

Finally, it has become increasingly obvious to me (and I believe to the rest of the committee) that the future we see emerging before us, as a result of our participation in this study, has heavy implications for public education. In a way, developing an informed and sophisticated public is what regional databases and their analyses and reports are all about. The burden of these education efforts may fall primarily upon health database organizations, but in my view this responsibility belongs to all interested parties, institutions, and professions. The purpose of these new information technologies is to enhance the health status of society and to improve health care for the individual patient. We hope and trust that this report itself will contribute to public understanding of these complex but important matters.

Roger J. Bulger, M.D., F.A.C.P.
Chair

Contents

Summary

An Institute of Medicine (IOM) study committee has examined the potential that existing and emerging health database organizations offer in improving the health of individuals and the performance of the health care system. *Health Data in the Information Age: Use, Disclosure and Privacy* advances recommendations related to the public disclosure of quality-of-care information and the protection of the confidentiality of personal health information. The emergence of health database organizations—whether through national health reform, state legislative initiatives, commercial ventures, or local business, medical, and hospital association coalitions—provides the impetus to explore how such assembled patient-level health care information can be used appropriately.

THE PROBLEM

The desire to understand and improve the performance of the health system begets a need for better health data for several purposes: to assess the health of the public and patterns of illness and injury; identify unmet regional health needs; document patterns of health care expenditures on inappropriate, wasteful, or potentially harmful services; identify cost-effective care providers; and provide information to improve the quality of care in hospitals, practitioners' offices, clinics, and other health care settings.

This, in turn, motivates proposals for the creation and maintenance of comprehensive, population-based health care databases that can provide such information with ease and reliability. Considerable obstacles lie in the way of achieving these goals. Some relate to the content and structure of current health databases; others concern the difficulties and costs of creating and maintaining comprehensive databases. Furthermore, public health databases (e.g., those maintained by states) may themselves lack connections with one another. Other problems include the need to create longitudinal records to understand how patients fare "in the system as a whole"; the need to adjust for important characteristics about patients' sociodemographic circumstances or health status (risk and severity adjustment); and the need to have information on the health of the population as a whole, not just of those who use the health system. Finally, the need for information on both end results (the outcomes) of care as well as on the processes of care poses great challenges to database developers.

The current push for health care reform has made clear to many that the success of reform options—as well as the ability to assess the effect of a reformed system on the health of the public—depends on access to the kinds of data that too often are unavailable.

Finally, as the reasons for creating large health databases mount, so do the possibilities that such databases (or, more correctly, their users) will do harm to patients, providers (institutions, physicians, and others), payers (government, private insurers, and corporations), and the public at large. The balance between the advantages of such databases and their potential for harm, or at least unfairness, to some groups is not yet clear, and the question of whether and how such entities ought to evolve has not been explored.

Recently, diverse groups of researchers, business leaders, and policymakers at state and regional levels have begun to develop databases intended to overcome some of the problems cited above and to permit increasingly sophisticated analyses of community health needs, practice patterns, costs, and quality of care. The interests that have prompted such action cover a broad range: the need to control business

costs attributable to health benefits, the desire to use technological and computer applications to decrease administrative costs of processing insurance claims, the wish of experienced health services researchers to exploit the potential of health databases to evaluate and improve health care, the responsibility of community leaders to plan expansion and contraction of health care facilities and services across the nation, and the need to maintain medical history information for an increasingly mobile population.

Coincident with these interests are the greatly enhanced electronic capabilities for data management in many aspects of daily life. Comprehensive computer-based health data files can be easily linked and information from those files moved instantaneously. Many observers believe that an unparalleled opportunity exists to apply computer technologies creatively to address many of the informational needs and data problems noted above. The report focuses on steps that might be taken to foster such action and progress through what the IOM committee terms *health database organizations*.

The committee uses *health database organization* (HDO) to refer to entities that have access to (and possibly control of) databases and a primary mission to publicly release data and the results of analyses done on the databases under their control. Although such entities do not yet exist, many are moving forcefully toward implementation. Prototypical HDOs have several characteristics; they

- operate under a single, common authority;
- acquire and maintain information from a wide variety of sources and put their databases to multiple uses;
- have files containing person-identified or person-identifiable data;
- serve a specific, defined geographic area;
- have inclusive population files;
- have comprehensive data with elements that include administrative, clinical, health status, and satisfaction information;
- manipulate data electronically; and
- support electronic access for real-time use.

For maximum accountability, protection, and control over access to person-identifiable data, HDOs will need an organizational structure, a corporate or legal existence, and a physical location. The value of HDOs and their databases might be said to be the timely provision of reliable and valid information to address all the major questions in health care delivery facing the nation today and in the coming years. The prospect of creating these entities has raised numerous issues, including (1) worries on the part of health care providers and clinicians about use or misuse of the information HDOs will compile and release, and (2) alarm on the part of consumers, patients, and their physicians about how well the privacy and confidentiality of personal health information will be guarded.

INSTITUTE OF MEDICINE STUDY

In early 1992 the IOM appointed a study committee to address these issues. The project took place during the 18 months before the Clinton administration introduced its Health Security Act in the fall of 1993; it was neither designed nor intended to reflect specifics of that or any of the other health care reform proposals that were debated beginning in late 1993. The study committee consisted of 16 individuals with expertise in administration of medical centers and academic health centers, the practice of medicine, administration of large (nonhealth) corporations, health insurance, utilization management, use of large administrative and research databases for research purposes, consumer services, health and privacy law, ethics, data security, informatics, and state health data organizations. In addition to meeting with experts in these areas and reviewing the literature, the committee conducted five major site visits;

it met with groups developing HDOs in business coalitions and other organizations, practicing physicians and representatives of local medical societies, insurers and third-party claims administrators, health maintenance organizations, consumers, hospital administrators and hospital associations, researchers, state and county health officials, employers, and computer system developers. At the conclusion of the study, the report underwent formal external review following the procedures of the National Research Council and the IOM.

The IOM committee took as a given that a variety of HDOs were being created and moving into operational phases and focused on two primary issues. The first is public release of descriptive and evaluative data on the costs, quality, and other attributes of health care institutions, practitioners, and other providers. The second involves the risks to and opportunities for protecting the privacy and confidentiality of data that do (or may) identify individuals in their role as patients or consumers, not as clinicians or providers.

USES AND USERS OF INFORMATION IN HDOs

Chapter 2 examines users and uses of HDO data and issues related to data quality. The major users of HDOs include health care provider organizations and practitioners, patients, their families, community residents, academic and research organizations, payers and purchasers, employers, health agencies, and others. The committee emphasizes that HDOs ought not necessarily to satisfy all such claimants. It does acknowledge, however, that the mere existence of a database creates new demands for access and new users and uses. Consequently, those who establish health databases and HDOs may be creating something for which the end uses cannot always be anticipated. Large databases such as those maintained by HDOs will be dynamic; in the committee's view, policies regarding access to those databases should, therefore, be based on firm principles that are flexible enough to accommodate unavoidable changes and unanticipated uses.

Databases

A *database* is "a large collection of data in a computer, organized so that it can be expanded, updated, and retrieved rapidly for various uses." Although databases may eventually be linked (or linkable) to primary medical records held by health care practitioners, the report addresses databases composed of secondary records that are generated subsequent to the primary record or that are separate from any patient encounter. They are not intended to be *the* major source of information about specific patients for the treating physician. The committee was particularly interested in linked databases that have, at a minimum, two specific characteristics: (1) their linking involves movement of health data outside the care setting in which they have been generated and (2) they include person-identified or person-identifiable data.

Key Attributes of Databases

In reviewing the considerable variation in databases that might be accessed, controlled, or acquired by HDOs, the committee sought a simple way to characterize them by key attributes. It selected two critical dimensions of databases: *comprehensiveness* and *inclusiveness*.

Comprehensiveness. Comprehensiveness describes the completeness of records about patient care events. It refers to the amount of information one has on an individual both for each patient encounter

with the health care system and for all of a patient's encounters over time.

Inclusiveness. Inclusiveness refers to which populations in a geographic area are included in a database. The more *inclusive* a database, the more it approaches coverage of 100 percent of the population that its developers intend to include. Databases that aim to provide information on the health of the community ought to have an enumeration of all residents of the community (e.g., metropolitan area, state) so that the information accurately reflects the entire population of the region, regardless of insurance category. Conversely, *inclusiveness* is reduced when membership is restricted to certain subgroups or when individuals expected to be in the database are missing.

Databases may be (and often are) designed to include only subsets of the entire population of a geographic area. The potential benefits of the database, however, will increase as the database moves toward being inclusive of the entire population of a defined geographic area.

Other Characteristics of Databases

The more comprehensive and inclusive they are, the more databases facilitate detailed and sophisticated uses. In turn, these attributes entail both greater anticipated benefits and possible harms. Factors determining the magnitude of either benefits or harms can depend on several properties of databases in addition to comprehensiveness and inclusiveness. Among the more important characteristics are linkage over time; the accuracy and completeness of data; whether the databases are under public- and private-sector control; and their origin (e.g., hospital discharge abstracts, self-completed questionnaires from patients, insurance claims, computer-based pharmacy files, computer-based patient records).

For purposes of this report, *person-identified data* contain pieces of information or facts that singly or collectively refer to one person and permit positive (or probable) identification of that individual. An obvious piece of identifying information is an individual's name. Other identifiers may be biometric, such as a fingerprint, a retinal print, or a DNA pattern. The committee uses *person-identifiable* to characterize information that definitely or probably can be said to refer to a specific person. It includes items of information (e.g., the fact of a physician visit on a given day) that will allow identification of an individual when combined with other facts (e.g., zip code of residence, date of birth, or gender). To render data non-person-identifiable, some data managers convert facts to a more general form before releasing those data to others. Concerns with person-identifiable data arise because of the ability of computers to combine and cross-match data in various databases. It is thus the more inclusive of these terms.

Throughout its discussions, the committee focused on *regional* databases--those that pertain to a *defined population* of individuals living in, or receiving health care in, some *specifiable geographic area*. Far-thinking experts envision a time when regional entities will be linked across the nation, even if their governance and operations remain close to home; this creates the very long-range view of a national health data repository (operated by either a single organization or a consortium of regional or state entities) as a federation of functionally linked databases from all regions of the country. Some proposed and developing HDO models are based on state legislation that requires submission of health data to a public agency. Other models are based on voluntary community cooperation and may be based on provider or local business coalitions.

Ensuring the Quality of Data

The real rewards from the development and operation of HDOs will depend heavily on the quality of their data, which must be reliable and valid for their intended purposes. Developers must ensure that the data in their systems are of high enough quality that analyses can be done in a credible, defensible manner. Success in meeting this responsibility will call for attention to the reliability, completeness, and accuracy of the data. Although the federal government may have to take the lead in standards development and improved coding systems, the committee urges HDOs to encourage and work toward national standards for coding and definitions for core data elements. Finally, the basic structure and content of these databases ought to be carefully designed from the beginning, but they must have sufficient capacity for expansion and change to accommodate the health care sector as it evolves in coming years.

To address these issues, the committee recommends that HDOs take responsibility for assuring data quality on an ongoing basis and, in particular, take affirmative steps to ensure: (1) the completeness and accuracy of the data in the databases for which they are responsible and (2) the validity of data for analytic purposes for which they are used (Recommendation 2.1, see Box S-1).

The absence of sufficient clinical information in most databases today leads investigators to acquire needed information through manual abstraction of relevant information in hospital records, but this approach is costly and time-consuming. Some means are needed to obtain this information more directly from patient records. The best method of enhancing the comprehensiveness of HDO databases and the accuracy and completeness of data elements is to move toward a computer-based patient record (CPR. This is admittedly a daunting task. Accordingly, the committee recommends that HDOs support and contribute to regional and national efforts to create computer-based patient records (Recommendation 2.2) including the development and adoption of relevant standards.

PUBLIC DISCLOSURE OF DATA ON HEALTH CARE PROVIDERS AND PRACTITIONERS

Chapter 3 examines public disclosure of data on health care practitioners and providers and presents recommendations about how HDOs can ensure that such analyses are fair to those identified and to the public. HDOs are presumed to have two major capabilities. One is the ability to amass credible descriptive information and evaluative data on costs, quality, and cost-effectiveness for hospitals, physicians, and other health care facilities, agencies, and providers. The other is the capacity to analyze data to generate knowledge and then to make that knowledge available for purposes of controlling the costs and improving the quality of health care—that is, of obtaining value for health care dollars spent. The committee characterizes the activities that HDOs might pursue to accomplish these goals as *public disclosure*, defined as the timely communication, or publication and dissemination, of certain kinds of information to the public at large. The aims are to improve the public's understanding about health care issues generally and to help consumers select providers of health care.

The committee stance favoring public disclosure takes two forms. One is that the HDOs ought *themselves* to carry out some minimum number of consumer-oriented studies and analyses and publish them routinely. The other is that HDOs must make appropriate data available for *others* to use in such studies and analyses, where the expectation is that the results of such work will be publicly disclosed.

Acceptance of HDO activities and products relating to public disclosure over time will depend in part on the balance struck for fairness to patients, the public in general, payers, and health care providers. Fairness to patients involves protecting their privacy and the confidentiality of information about them. Fairness to the public involves distributing the accurate and reliable information needed to

make informed decisions about providers and health care interventions. Finally, fairness to providers entails ensuring that data and analyses are reliable, valid, and impartial, giving providers some opportunity to confirm data and methods before information is released to the public, and finding some means of publishing their perspectives when it is released.

Key Factors in Public Disclosure

Public disclosure is acceptable *only* when it (1) involves information and analytic results that come from studies that have been well conducted, (2) is based on data that can be shown to be reliable and valid for the purposes at hand, and (3) is accompanied by appropriate educational material.

Several elements are crucial to successful public disclosure of health-related information. Among the more significant are topics of analysis (e.g., hospital-specific death rates) and who is identified in such releases (e.g., health plans, institutional providers, and individual practitioners). The full report explores these matters in some detail.

In the committee's view, disclosure of information about larger aggregations of health care providers, such as hospitals, will generally be less prone to cause undeserved losses of reputation, income, or career than disclosure of information on specific individual practitioners. The committee takes the position that public disclosure is a valuable goal to pursue, to the extent that it is carried out with due attention to accuracy and clarity and does not undermine the quality assurance and quality improvement (QA/QI) programs that health care institutions and organizations conduct internally.

Analyses and Disclosure of Results

The committee recommends that HDOs produce and make publicly available appropriate and timely summaries, analyses, and multivariate analyses of all or pertinent parts of their databases. More specifically, the committee recommends that HDOs regularly produce and publish results of provider-specific evaluations of costs, quality, and effectiveness of care (Recommendation 3.1).

The subjects of such analyses should include hospitals, health maintenance organizations, and other capitated systems; fee-for-service group practices of all sorts; physicians, dentists, podiatrists, nurse-practitioners, or other independent practitioners; long-term-care facilities; and other health providers on whom the HDOs maintain reliable and valid information.

The intended audience for publication or disclosure is the public, not simply member or sponsoring organizations. Some HDOs may be based in the private sector, operate chiefly for the benefit of for-profit entities, and have no connection with or mandate from states or the federal government. In these cases, the imperative to make information and analytic results available to the public on a broad scale is less clear. In the committee's view, however, the charters and bylaws of such HDOs ought to include firm commitments to conduct consumer-oriented studies, and where state legislation is used to establish HDOs or similar entities (e.g., data commissions), the enabling statutes themselves should contain such requirements. If public funds are used to support the development of HDOs, public release of analyses should be required as a condition of funding.

Describing Analytic Methods

The committee recommends that an HDO report the following for any analysis it releases publicly:

- general methods for ensuring completeness and accuracy of data;
- a description of the contents and the completeness of all data files and of the variables in each file used in the analyses;
- information documenting any study of the accuracy of variables used in the analyses (Recommendation 3.2).

The committee expects HDOs to accompany public disclosure of provider-specific information with clear descriptions of the database (including documentation of its completeness, accuracy, and data sources), of methods of risk adjustment, and of appropriate uses by the public, payers, and government of the data and analyses--including notice of those uses of data and analyses that are *not* valid.

Minimizing Potential Harms

The committee has taken a strong pro-disclosure stance toward comparative, evaluative data. Disclosure proponents assume that such studies will be done responsibly, and the public has every right to expect that to be the case. The committee sees some potential for harm in public release of comparative or evaluative studies on costs, quality, or other measures of health care delivery, however, and did not wish to rely solely on marketplace correctives; it believes that a more protective stance is needed. To enhance the fairness and minimize the risk of unintended harm from the publication of evaluative studies that identify individual providers, the committee recommends that each HDO should adhere to two principles as a standard procedure prior to publication: (1) to make available to and upon request supply to institutions, practitioners, or providers identified in an analysis all data required to perform an independent analysis, and to do so with reasonable time for such analysis prior to public release of the HDO results; and (2) to accompany publication of its own analyses with notice of the existence and availability of responsible challenges to, alternate analyses of, or explanations of the findings (Recommendation 3.3). Feedback from providers may reveal problems with data quality and study methods that HDOs would want to remedy. This set of recommendations reflects what might be regarded as a fairness doctrine.

Releasing Data

HDOs might well serve as a major repository of data that will be accessible to other groups. To foster the presumed benefits of widespread applications of HDO data, the committee recommends that HDOs should release non-person-identifiable data upon request to other entities once those data are in analyzable form. This policy should include release to any organization that meets the following criteria:

- It has a public mission statement indicating that promoting public health or the release of information to the public is a major goal.
- It enforces explicit policies regarding protection of the confidentiality and integrity of data.
- It agrees not to publish, redisclose, or transfer the raw data to any other individual or organization.
- It agrees to disclose analyses in a public forum or publication.

The committee also recommends, as a related matter, that HDOs make public their own policies governing the release of data (Recommendation 3.4).

STRENGTHENING QUALITY ASSURANCE AND QUALITY IMPROVEMENT PROGRAMS THROUGH DATA FEEDBACK

HDOs could help to improve the quality of health care through direct assistance to health care institutions, facilities, and clinical groups by making available to providers and practitioners the data for or results of evaluative studies of their services and those of their peers.

The committee assumed such an activity would occur chiefly as a part of or as an adjunct to a formal QA/QI process that providers and plans might conduct. Information on identified providers and individual clinicians would be made available to organizations' QA/QI programs so that they could take constructive action.

Some readers may think that a tension will exist between public disclosure and such feedback for internal use, but the committee believes that both will be important tools available to HDOs to improve quality and foster informed choices in health care. Thus, it voices support for both functions, in the belief that one activity does not–or at least need not–discredit the other and that effective combination strategies can be designed.

CONFIDENTIALITY AND PRIVACY OF PERSONAL DATA

Chapter 4 of the IOM report examines privacy, confidentiality, and security of information about individuals or patients–what this committee refers to as person-identified or person-identifiable data.

Two somewhat distinct trends have led to increased access to the primary health record and subsequent concerns about privacy. One has to do with primary health records, however they are created and maintained, and the other involves health records stored electronically.

The increasing complexity of health care and the involvement of greater numbers of individuals in health care delivery has resulted in ever more people accessing the health record to deliver and document care. The primary health record serves many purposes beyond direct health care, and many parties external to the healing relationship seek person-identified information. Of particular concern is the confidentiality of health information that is stored electronically; the aggregation of information on individuals from diverse databases will make computer-based health data increasingly valuable and in need of protection from unauthorized access.

Existing ethical, legal, and other approaches to protecting confidentiality and privacy of personal health data offer some confidentiality safeguards, but major gaps and limitations remain. The committee's recommendations are intended to strengthen current protections for confidentiality and privacy of health-related data, particularly for information acquired by HDOs.

Privacy and Privacy Rights

The most general and common view of privacy conveys notions of withdrawal, seclusion, secrecy, or of being kept away from public view, but with no pejorative overtones. In public policy generally, and in health policy in particular, privacy takes on a special meaning, namely, that of *informational privacy*, "a state or condition of controlled access to personal information." Informational privacy is infringed, by definition, whenever another party has access to one's personal information by reading, listening or using any of the other senses. Such loss of privacy may be entirely acceptable and intended by the individual, or it may be inadvertent, unacceptable, and even unknown to the individual.

This definition of privacy thus reflects two underlying notions. First, privacy in general and

informational privacy in particular are always matters of degree. Rarely is anyone in a condition of complete physical or informational inaccessibility to others, nor would they wish to remain so. Second, although informational privacy may be valuable and deserving of protection, many thoughtful privacy advocates argue that it does not, in itself, have moral significance or inherent value.

Nonetheless, informational privacy has value for all in our society, and it accordingly has special claims on our attention. The most salient federal protections for privacy are the principles of fair information practices embodied in the Privacy Act of 1974. The act addresses the right to know about, challenge, control, and correct information about oneself in federal government databases.

Privacy Rights

No explicit right to privacy is guaranteed by the Constitution of the United States. The presumed right as the basis of a civil action is based on legal opinion written by Justice Louis D. Brandeis in 1890, and its constitutional status derives from various amendments to the Bill of Rights. The Constitution generally has not provided strong protection for the confidentiality of individual health care information; the constitutional protection for informational privacy is very limited and derived from case law interpreting the Constitution.

To assert a right is to make a special kind of claim. Rights designate some interests of the individual that are sufficiently important to hold others under a duty to promote and protect, sometimes even at the expense of maximizing or even achieving the social good. Two interests are widely cited as providing the moral justification for privacy rights: the individual's interest in autonomy and the instrumental value that privacy may have in promoting other valuable human goods.

Whether HDOs can achieve their potential for good in the face of their possible impact on privacy will likely turn on the interplay of three considerations. First, to what extent do HDOs provide important (and perhaps irreplaceable) health care benefits to the regions in which they operate, and perhaps to the nation? Second, how will adequate privacy safeguards be incorporated into the HDOs? Third, do the societal benefits resulting from the implementation of HDOs outweigh the privacy risks?

There cannot be much doubt that HDOs will serve legitimate societal interests. Nevertheless, because HDOs will represent one of the more comprehensive and sensitive automated personal record databases yet established, the system inevitably implicates interests protected by informational privacy principles.

Confidentiality

Confidentiality relates to disclosure or nondisclosure of information. Historically, a duty to honor confidentiality has arisen with respect to information disclosed in the context of a relationship such as that between a physician and a patient. When one is concerned about data disclosure, whether or not any relationship exists between a data subject and a data holder, an essential construct is that of *data confidentiality*. It is the status accorded data indicating that they are protected and must be treated as such.

Exceptions to confidentiality requirements are widely acknowledged. Situations exist in which sensitive health information about individuals must be disclosed to third parties. Such reporting requirements are justified by society's need for information. Examples include mandatory reporting of communicable diseases and gunshot wounds. Physicians and other health professionals may also be required to divulge personal health information under legal "compulsory process," which may take the form of subpoenas or discovery requests enforced by court order.

The most important exception to the rule of confidentiality, however, is that of disclosure

authorized by consent of a patient or a patient representative in the course of applying for insurance, employment, or reimbursement for medical claims. Such disclosure may or may not be justifiable and acceptable to patients. In such a case, however, consent cannot be truly voluntary or informed. Such authorizations are often not *voluntary* because the patient feels compelled to sign the authorization or forego the benefit sought, and they are not *informed* because the patient cannot know in advance what information will be in the record, who will subsequently have access to it, or how it will be used. Although such consent procedures are a necessary adjunct to other autonomy protections, this committee generally does not regard these procedures as sufficient in themselves to protect sensitive information from inappropriate disclosure.

Legal and ethical confidentiality obligations are the same whether health records are kept on paper or computer-based media. Current laws, however, have significant weaknesses. First, and very important, the degree to which confidentiality is required under current law varies according to the holder of the information and the type of information held.

Second, legal obligations of confidentiality often vary widely within a single state and from state to state, making it difficult to ascertain the legal obligations that a given HDO will have, particularly if it operates in a multistate area. These state-by-state and intrastate variations and inconsistencies in privacy and confidentiality laws are well established among those knowledgeable about health care records law; they are worrisome because some HDOs will routinely transmit data across state lines.

Third, current laws offer individuals little real protection against redisclosure of their confidential health information to unauthorized recipients for a number of reasons. Once patients have consented to an initial disclosure of information (for example, to obtain insurance reimbursement), they have lost control of further disclosure. Information disclosed for one purpose may be used for unrelated purposes without the subject's knowledge or consent. Such redisclosure practices represent a yawning gap in confidentiality protection.

As a practical matter, policing redisclosure of one's personal health information is difficult and may be impossible. At a minimum, such policing requires substantial resources and commitment. With the use of computer and telecommunications networks, an individual may never discover that a particular disclosure has occurred, even though he or she suffers significant harm--such as inability to obtain employment, credit, housing, or insurance--as a result of such disclosure. Pursuing legal remedies may result in additional disclosure of the individual's private health information.

Further, federal law may preempt state confidentiality requirements or protections without imposing new ones. For example, the Employment Retirement Insurance Security Act (ERISA) preempts some state insurance laws with respect to employers' self-insured health plans, yet ERISA is silent on confidentiality obligations.

Last, enforcing rights through litigation is costly, and money damages may not provide adequate redress for the harm done by the improper disclosure. In addition, suing for privacy invasion may require further exposure of sensitive information to the public.

Security

In the context of health record information, confidentiality implies controlled access to and protection against unauthorized access to, modification of, or destruction of health data. In computer-based or computer-controlled systems, security is implemented when a defined system functions in a defined operational environment, serves a defined set of users, contains prescribed data and operational programs, has defined network connections and interactions with other systems, and incorporates safeguards to protect the system against a defined threat to the system, its resources, and its data.

Two consequences flow from defining data as sensitive and needing protection. First, those data must be made secure; second, access must be controlled. Access control can be operationalized by HDO planners and legislators in a form that this committee would term "information-use policy." It leads to policymaking about who may be allowed to use health-related information and how they may use it. It might also include consideration of whether some data should be collected at all.

In a study that focuses on the protection of health-related data about individuals, defining which items are health-related is more difficult than one might initially think. Any data element in medical records, and many data items from other records, *could* be considered either health-related or sensitive, or both. In considering the actions of HDOs, this committee proceeds from an assumption that *all* information concerning an individual and any transactions relating directly or indirectly to health care that HDOs access or maintain as databases must be regarded as potentially requiring privacy protections.

A National Identification System or Dossier

HDOs may be perceived as enabling the development of a national identification system or dossier. Privacy advocates can be expected to express acute concern about the potential for HDOs to be linked not only with one another, but, more importantly, with government databases and with other personal databases such as the financial, credit, and lifestyle databases maintained by consumer reporting agencies. The committee believes that HDO proponents should take every practicable step, including those recommended by the committee, to assure that HDOs will not contribute to the development of a national identification database.

Personal Identifiers and the Social Security Number

The personal identifier (ID) that is used in an HDO to "label" each of the individuals on whom it keeps data is a crucial issue. It not only is related to past practices, but it will also be strongly influenced, if not mandated, by the health care reform actions now under way in the nation.

An "Ideal" Identifier

The choice of a personal ID that is satisfactory for the operational needs of health care delivery but at the same assures the confidentiality of medical data and the privacy of individuals is neither easy nor casual. An ideal identifier would meet the requirements described in detail in the report. Superficially, the choice would be the Social Security number (SSN), Medicare number, or something similar simply because people are accustomed to using them, systems are used to handling them, and the government would bear the burden of administering the enumeration system and the cost of assigning new numbers. The SSN has many faults, however, that are familiar to researchers and privacy experts. Perhaps the most salient of these is that if the SSN were to become the ID for health care delivery, linkage of medical records to all the other databases would become easy.

The most problematic objection to the SSN as a medical ID is that it has no legal protection, and because its use is so widespread, there is no chance of retroactively giving it such protection. As a data element, it is not characterized by law as confidential; hence, organizations holding it are under no legal requirement to protect it or to limit the ways in which it is used. Its use is for all practical purposes unconstrained, and this makes the risk of commingling health data with all other forms of personal data and an individual's actions extremely high. Major privacy risks arise when medical information is used

in decisions unrelated to health care, such as employment, promotion, and eligibility for insurance or other benefits. Further, access by unauthorized users would be very much simpler because the SSN is so readily available.

Relevance to HDOs of Existing Laws on Confidentiality and Privacy

The committee examined existing law—constitutional, statutory, and common law—for its relevance to HDOs and its adequacy for protecting patient privacy and confidentiality. The committee also examined the way these laws might affect the design, establishment, and operation of HDOs.

It concludes that most of this body of law is unlikely to apply to HDOs. With the exception of laws that regulate certain information considered sensitive, existing laws regulate recordkeepers and their recordkeeping practices; they do not regulate on the basis of either the content or the subject matter of a record.

Recommendations Regarding Protection of Patient and Person-identifiable Data

Given (1) the unprecedented comprehensiveness and inclusiveness of information expected to be in HDO databases, (2) the generally scanty and inconsistent legal protections across geopolitical jurisdictions, and (3) the current public interest in and concern about privacy protections, the committee believes that HDOs have both an obligation and an opportunity to fashion well-delineated privacy protection programs that will also foster the realization of HDO goals. Some of these protections, such as the establishment of data protection boards and organizational policies regarding security and access control, can be implemented in the short term. Others, such as passage of federal preemptive legislation, will likely require longer-term efforts.

Preemptive Legislation

The committee recommends that the U.S. Congress move to enact preemptive legislation that will:

- establish a uniform requirement for the assurance of confidentiality and protection of privacy rights for person-identifiable health data and specify a Code of Fair *Health* Information Practices that ensures a proper balance among required disclosures, use of data, and patient privacy;
- impose penalties for violations of the act, including civil damages, equitable remedies, and attorney's fees where appropriate;
- provide for enforcement by the government and permit private aggrieved parties to sue;
- establish that compliance with the act's requirements would be a defense to legal actions based on charges of improper disclosure; and
- exempt health database organizations from public health reporting laws and compulsory process with respect to person-identifiable health data except for compulsory process initiated by record subjects (Recommendation 4.1).

In the last item, the committee believes that both processes—public health reporting and

responding to compulsory process such as subpoenas—should remain the responsibility of the provider, as is now the case.

The committee concludes that federal preemptive legislation is required to establish uniform requirements for the preservation of confidentiality and protection of privacy rights for health data about individuals. It further advises that Congress enact such legislation, including a Code of Fair *Health* Information Practices, as soon as possible. At a minimum, federal legislation should establish a floor and allow states or HDOs to implement more stringent standards so that state-imposed safeguards are not weakened.

Although current state protections often apply duties of confidentiality to the recordkeeper (e.g., the hospital), such protection is no longer in effect once the data have left the recordkeeper's control. This means that health data can be deprived of legal protection unless such protection is specified by another law; furthermore, such protection is likely to be left to the discretion of organizations or individuals who acquire such information as secondary data. That is little shelter indeed. Therefore, legislation should clearly establish that the confidentiality of person-identifiable data is a property afforded to the data elements themselves, regardless of who holds those data. Proper preemptive legislation should also provide for enforcement by government officials and aggrieved private parties. It should also impose penalties for violations of the act. It will be important that the legislation clarify whether individuals have standing to bring suit.

Federal legislation can be expected to encourage standard setting in such areas as connectivity and transmissions standards. Standard setting is a major obstacle to the development of automated medical records and will be no less a problem for HDOs. Thus, the committee sees the route of federal legislation as one more mechanism for addressing this problem for all computer-based systems that deal with health data.

Data Protection Units

HDOs will need clear and enforceable, written organizational policies and procedures in several areas: informing patients of their rights regarding their own data; protecting medical information and materials; ensuring the accuracy of data; and verifying compliance with their policies. Members of the public should be able to request and receive clearly written materials describing these policies. Although precise policies cannot be written to cover every eventuality, they must be broad enough to address the most common situations, such as types of data and potential requestors. Organizations should also make considerable efforts to educate (and reeducate) staff, the public, and potential requestors about these policies. Thus, the committee recommends that HDOs establish a responsible administrative unit or board to promulgate information policies concerning the acquisition and dissemination of information and to establish whatever administrative mechanism is required to implement these policies. Such an administrative unit or board specifically should:

- promulgate and implement policies concerning data protection and analyses based on such data;
- develop and implement policies that protect the confidentiality of all person-identifiable information, consistent with other policies of the organization and relevant state and federal law;
- develop and disseminate educational materials for the general public that will describe in understandable terms the analyses and their interpretation of the rights and responsibilities of individuals and the protections accorded their data by the organization;
- develop and implement security practices in the manual and automated data processing and storage systems of the organization; and

- develop and implement a comprehensive employee training program that includes instruction concerning the protection of person-identifiable data (Recommendation 4.2).

The commitment to protection of confidentiality of the governing body and executives of the HDO will be critical, and these objectives should be written into the organization's bylaws. The committee strongly advises that HDO policy boards include in their policies and procedures fair health information practices. Any HDO should consider these practices as the foundation of its privacy framework and depart from them only after careful consideration and explanation.

Legislation and organizational policies have sometimes distinguished among levels of sensitivity of various elements of health-related data, based on the belief that it is possible to identify categories of data that warrant special protection. Despite precedent for adopting such a stance, this committee has decided otherwise. It has concluded that a given data element cannot always be designated reliably as inherently sensitive; rather, the sensitivity of data depends on the kinds of harm to which individuals are or believe themselves to be vulnerable if the information were known to others. Such assessments could differ dramatically from one person to another, one circumstance to another, one place to another, and over time as cultural attitudes change. Rather than recommending special protections for certain categories of data, the committee prefers that all data accessed by HDOs be afforded stringent, and essentially equal, protection.

Release of Person-Identified Data

Policies Relating to Access and Disclosure

Clearly, the question of who *outside* the HDO has access to what data, and under what circumstances, is supremely important and is the essence of the privacy issue from the patient's point of view. The committee takes up these matters in a series of recommendations (presented below) that refer to person-identified or person-identifiable information only. As discussed earlier in this summary, the committee recommends release and disclosure of nonperson-identifiable information that protects patient identity but that provides reliable, valid, timely, and useful descriptive and evaluative information on a full range of health care providers and clinicians.

The committee recognizes that there must be release of patient-identified data related to the processing of health insurance claims. The committee recommends, however, that a health database organization *not* release person-identifiable information in other circumstances *except* the following:

- to other HDOs whose missions are compatible with and whose confidentiality and security protections are at least as stringent as their own;
- to individuals for information about themselves;
- to parents for information about a minor child except when such release is prohibited by law;
- to legal representatives of incompetent patients for information about the patient;
- to researchers with approval from their institution's properly constituted institutional review board;
- to licensed practitioners with a need to know when treating patients in life-threatening situations who are unable to consent at the time care is rendered; and
- to licensed practitioners when treating patients in all other (non-life-threatening) situations, *but only with the informed consent of the patient.*

Otherwise, the committee recommends that health database organizations not authorize access to, or release of, person-identifiable information with or without informed consent (Recommendation 4.3).

In the last item, the committee has specifically recommended that consent for access to the database be a necessary and sufficient condition in only one circumstance: when needed by the treating practitioner in non-life threatening situation. In such a situation it will be important that specific consent mechanisms be in place. Otherwise, the committee believes that informed consent should *not* be required for release of person-identifiable information in six situations as described below.

First, HDOs will need to acquire information about out-of-area care provided to persons in their databases and should be able to do so. Second, HDOs also ought to release person-identifiable data without requiring consent when individuals seek information about themselves. The third and fourth cases above reflect the need to care for minors and persons who are legally incompetent to give consent for themselves.

The fifth case concerns researchers with approval from relevant human subjects committees or institutional review boards (IRBs). In this case, person-identified information is not being sought *by* a patient or *for care of* a patient, but to conduct studies that are regarded as being in the public's interest. Such uses of the databases are considered by this committee to be central and vital to the effective implementation of HDOs.

The sixth case involves treatment of licensed practitioners with a need to know in life-threatening situations, whom the committee believes also ought to be able to access data about a patient. This requires that the patient be unable to consent at the time care is rendered.

The seventh case–the release of data to licensed practitioners when treating patients in all other (non-life-threatening) situations, but only with the informed consent *of the patient*–is the only case in which the committee has recommended the use of informed consent to release of person-identifiable information. Such a circumstance might occur when a treating physician wishes to access the HDO database in addition to the medical records he or she keeps. For example, information on medications prescribed by other practitioners might be pertinent. In such cases, the treating practitioner should obtain explicit consent of the patient. As discussed earlier, consent might be given electronically and might be time limited.

Finally, the committee recommends above that HDOs *not* authorize access to or release of health information on individuals *with or without the informed consent* of the individual in any situation or to any requestor other than those stated above. To ensure that individuals (i.e., patients, parents of minor children, or patients' legal representatives) are not placed in an untenable situation concerning release information, the committee has opted for a position that does not rely on consent procedures insofar as most uses or disclosures of data are concerned. It prefers to rely on stringent policies against disclosure or release of personal information on individuals. The consent procedures described in this recommendation are for release of information by the HDO. Patients will always be able to consent to release of information directly by each of their care providers.

Special circumstances exist in the health sector that are of particular concern to the committee. One involves the current practice of extensive exchange of medical information between employer and payer with little control by providers or patients. This practice has dramatic implications for patients whose information is accessed by an HDO if the employer and payer are readily able to tap into data in the network. Such exchanges of information could be especially harmful to patients because the information exchanged could cover all encounters the patient has with the health care system (not just those covered by insurance or by the employer's health plan). The committee acknowledges the danger and inappropriateness of these practices and regarded them as sufficiently worrisome that it recommends that employers not be permitted to require receipt of an individual's data from a health database organization as a condition of employment or for the receipt of benefits (Recommendation 4.4).

Universal Person-Identifiers

The committee believes that unique individual person-identifiers are essential to facilitate the efficient operation and data interchange of HDOs. The committee also recognizes that there are strong arguments against the SSN being used as the unique identifier. The great majority of the committee agreed on the need for a new unique identifier on the grounds that the SSN offers too many opportunities to breach confidentiality. The creation of a new number would (1) permit legislative protection of that number, (2) offer the possibility of providing greater protection for health information than is possible with the SSN, and (3) likely occur at the time of implementation of universal health care coverage, which will, in any case, require some scheme for unique identification.

THE FUTURE

Little is yet known about how HDOs will function, what will be their likely benefits, or how they will evolve over time. In emphasizing the use of aggregated health information, the Clinton Administration's health reform proposal has put the issue of confidentiality squarely on the agenda. What is not known is which uses of health care information will be acceptable and will wisely serve the needs of society. Moreover, new uses for and users of data will emerge, some raising new threats to privacy. Accordingly, the privacy dimension of health care information is dynamic and should be revisited from time to time.

Regional HDOs hold tremendous promise for evaluating and improving health care and implementing effective new ways to protect health information. Although the great public benefit may be easily understood, the potential for harm or lack of fairness may create concern and fear in many. To gain public support for the vision advanced in this report—and to ensure the best public use of the health-related information that will be released—HDOs, government agencies, and public- and private-sector institutions must implement carefully planned strategies for fairness and privacy protection and educate the public, health care providers, policymakers, and patients about these protections. This report is intended to be an early step in that educational and public policy-making process.

BOX S-1 COMMITTEE RECOMMENDATIONS

RECOMMENDATION 2.1 ACCURACY AND COMPLETENESS

To address these issues, the committee recommends that health database organizations take responsibility for assuring data quality on an ongoing basis and, in particular, take affirmative steps to ensure: (1) the completeness and accuracy of the data in the databases for which they are responsible and (2) the validity of data for analytic purposes for which they are used.

Part 2 of this recommendation applies to analyses that HDOs conduct. They cannot, of course, police the validity of data when used by others for purposes over which the HDOs have no a priori control.

RECOMMENDATION 2.2 COMPUTER-BASED PATIENT RECORD

Accordingly, the committee recommends that health database organizations support and contribute to regional and national efforts to create computer-based patient records.

RECOMMENDATION 3.1 CONDUCTING PROVIDER-SPECIFIC EVALUATIONS

The committee recommends that health database organizations produce and make publicly available appropriate and timely summaries, analyses, and multivariate analyses of all or pertinent parts of their databases. More specifically, the committee recommends that health database organizations regularly produce and publish results of provider-specific evaluations of costs, quality, and effectiveness of care.

RECOMMENDATION 3.2 DESCRIBING ANALYTIC METHODS

The committee recommends that a health database organization report the following for any analysis it releases publicly:

- general methods for ensuring completeness and accuracy of their data;
- a description of the contents and the completeness of all data files and of the variables in each file used in the analyses;
- information documenting any study of the accuracy of variables used in the analyses.

RECOMMENDATION 3.3 MINIMIZING POTENTIAL HARM

The committee recommends that, to enhance the fairness and minimize the risk of unintended harm from the publication of evaluative studies that identify individual providers, each HDO should adhere to two principles as a standard procedure prior to publication: (1) to make available to and upon request supply to institutions, practitioners, or providers identified in an analysis all data required to perform an independent analysis, and to do so with reasonable time for such analysis prior to public release of the HDO results; and (2) to accompany publication of its own analyses with notice of the existence and availability of responsible challenges to, alternate analyses of, or explanation of the findings.

RECOMMENDATION 3.4 ADVOCACY OF DATA RELEASE: PROMOTING WIDE APPLICATIONS OF HEALTH-RELATED DATA

To foster the presumed benefits of widespread applications of HDO data, the committee recommends that health database organizations should release non-person-identifiable data upon request to other entities once those data are in analyzable form. This policy should include release to any organization that meets the following criteria:

- It has a public mission statement indicating that promoting public health or the release of information to the public is a major goal.

Continued

- It enforces explicit policies regarding protection of the confidentiality and integrity of data.
- It agrees not to publish, redisclose, or transfer the raw data to any other individual or organization.
- It agrees to disclose analyses in a public forum or publication.

The committee also recommends, as a related matter, that health database organizations make public their own policies governing the release of data.

Recommendation 4.1 Preemptive Legislation

The committee recommends that the U.S. Congress move to enact preemptive legislation that will:

- establish a uniform requirement for the assurance of confidentiality and protection of privacy rights for person-identifiable health data and specify a Code of Fair Health Information Practices that ensures a proper balance among required disclosures, use of data, and patient privacy;
- impose penalties for violations of the act, including civil damages, equitable remedies, and attorney's fees where appropriate;
- provide for enforcement by the government and permit private aggrieved parties to sue;
- establish that compliance with the act's requirements would be a defense to legal actions based on charges of improper disclosure; and
- exempt health database organizations from public health reporting laws and compulsory process with respect to person-identifiable health data except for compulsory process initiated by record subjects.

Recommendation 4.2 Data Protection Units

The committee recommends that health database organizations establish a responsible administrative unit or board to promulgate and implement information policies concerning the acquisition and dissemination of information and establish whatever administrative mechanism is required to implement these policies. Such an administrative unit or board should:

- promulgate and implement policies concerning data protection and analyses based on such data;
- develop and implement policies that protect the confidentiality of all person-identifiable information, consistent with other policies of the organization and relevant state and federal law;
- develop and disseminate educational materials for the general public that will describe in understandable terms the analyses and their interpretation of the rights and responsibilities of individuals and the protections accorded their data by the organization;
- develop and implement security practices in the manual and automated data processing and storage systems of the organization; and
- develop and implement a comprehensive employee training program that includes instruction concerning the protection of person-identifiable data.

RECOMMENDATION 4.3 RELEASE OF PERSON-IDENTIFIED INFORMATION

The committee recognizes that there must be release of patient-identified data related to the processing of health insurance claims. The committee recommends, however, that a health database organization *not* release person-identifiable information in any other circumstances *except* the following:

- **to other HDOs whose missions are compatible with and whose confidentiality and security protections are at least as stringent as their own;**
- **to individuals for information about themselves;**
- **to parents for information about a minor child except when such release is prohibited by law;**
- **to legal representatives of incompetent patients for information about the patient;**
- **to researchers with approval from their institution's properly constituted Institutional Review Board;**
- **to licensed practitioners with a need to know when treating patients in life-threatening situations who are unable to consent at the time care is rendered; and**
- **to licensed practitioners when treating patients in all other (non-life-threatening) situations, *but only with the informed consent of the patient.***

Otherwise, the committee recommends that health database organizations not authorize access to, or release of, information on individuals with or without informed consent.

RECOMMENDATION 4.4 RESTRICTING EMPLOYER ACCESS

The committee recommends that employers not be permitted to require receipt of an individual's data from a health database organization as a condition of employment or for the receipt of benefits.

Mr. SAWYER. Thank you all very much.

I particularly want to express my gratitude to you for expressing the goal in terms of reducing cost escalation. There are just too many people in the course of this entire multi-year debate who have too often allowed listeners to walk away thinking that somehow they were going to get more and better for less, and that is simply not the case.

If we do our jobs well, we will hold the line and continue to provide a very high quality of health care to a larger number of people in this country without reducing the quality of what they get, and to do so without the kinds of cost escalations that we would predict without other kinds of intervention. If we can do that, we will have achieved a great deal, and then, perhaps, we can look for savings down the road. But, it's very important to understand that.

And, the kinds of information systems that we are talking about really go to the heart of what Senator Moynihan said 25 years ago. You can't solve a problem until you can measure it accurately. This really becomes the central nervous system for the entire range of very complex interactions among individuals and institutions and funding mechanisms that are our health care system.

What would be lost if the kind of access to Medicare and other kinds of medical information available today were curtailed in serious ways? Are the protections in place to safeguard the data adequately?

Ms. MOON. I think that the current safeguards that are there for Medicare are adequate. We may want to think about some additional safeguards when we are talking about a national health system, for the reason that Tom mentioned. That is, to get people's full cooperation in an environment where they are skeptical and, perhaps, even fearful of what you'll do with the information, you need to provide a lot of reassurance up front that there are protections.

We would lose a great deal if, however, in the enthusiasm to provide reassurance to people and protections we put so many barriers in place that you can not either obtain at a national level these very broad snapshots or link them back to other data.

What we'd find if we did that is in five years, when we are worried about costs, that we'll have to go back and reproduce data from scratch. That would be very expensive. I think there are also some really exciting opportunities to learn things about health care that we don't know. It is crucial to express to individuals the possibilities for improving health care from research using these data.

Mr. JUSTER. Can I just add, I guess as a general proposition I would say that the way to put the question is, what do you lose, and what is it that you have to safeguard if you do provide access, that is, what kind of risks of having inadvertent, unfortunate events like disclosures with consequences happening?

There, I would go back to the comment I made in the testimony. I think it is clearly in the interest of society to adopt a policy in which data which are collected and used for research and statistical purposes simply cannot be used for individual enforcement or individual administration. And, the reason I think that's such an important thing to put in place is that it has one of the—depending on which way you want to look at it, it has the largest benefit cost

ratio of virtually any policy I can think of, or the lowest cost benefit ratio, depending on which one you put on the top and which on the bottom, because the enforcement folks don't gain a thing that they don't already have. And, yet, the research people gain a lot by having a data collection that everybody knows who has done it is one of the more expensive aspects of the research project.

If you can minimize the cost of providing the right kind of database by selectively and judiciously accessing existing data from administrative records, provided you can safeguard people against the possibility that they are then at risk, you clearly ought to do it.

And, I think legislation to do this, you know, there are some agencies, some data sources, which are currently protected in that way, but that's not always true. I'm not sure about the medical, you know, I know the kinds that are, one of the ones I'm involved in, achieved that protected status, and it's very comforting to have that.

I don't think it applies generally to all types of records. It may or may not apply to the ones you are talking about. It's critical that it do apply to those, that you can assure people that they are not facing a risk.

Mr. SAWYER. That goes really to the question that you raised in your testimony about functional separation.

Mr. JUSTER. Exactly.

Mr. SAWYER. The Committee on National Statistics recommends an independent body. Do you all support that kind of approach? And, if so, should one entity be guaranteeing privacy and another access? Should it be a single body that comes to that judgment? How do you resolve that fundamental tension?

Mr. JUSTER. Let me make two comments about that. One is, I think it ought to be a body which doesn't have—you know, it ought to be representative of several types of points of view. There ought to be people on that body who are sensitive to privacy issues, medical ethicists. You ought to have people who are actively involved in the research process and like to broaden use. So, it ought to have tensions which exist in the body itself on both sides of that.

And, you know, quite frankly, I wouldn't trust researchers to make that final judgment. You can find lots of instances where the research community, because they are anxious to get the data, have over promised. I mean, I can cite you chapter and verse, and you know some yourself. It's not a good idea to have just folks who are advocates, they should be confronted with people who say, all right, well, what about the protection, what kind of guarantees, how critical is it, and they should pose hard questions.

I think the notion of an independent board, I think has got a lot going for it, and I don't see any reason why, I don't see any negatives, frankly.

Mr. SAWYER. Do you foresee institutional review boards coexisting with this, as a matter of proposing these things?

Mr. JUSTER. Yes, I would.

Mr. SAWYER. But, not making decisions about access.

Mr. JUSTER. That's the way I would do it, yes.

Mr. SAWYER. Any of the others have comments about that?

Dr. BULGER. I would certainly agree with that, because I really think if you separate the two functions, somebody, and some other committee, is going to have to integrate.

Mr. SAWYER. Right.

Dr. BULGER. And, it's really much more constructive to force them to integrate right off the bat.

Ms. MOON. I'd only add, that one of the considerations that should always be on the table is how timely these decisions will be. We don't want to set up a mechanism where you have appeals and long, lengthy processes before releasing the data, because one of the real goals of this kind of data is to be very timely. That should be put into the equation as well.

Mr. SAWYER. Almost anything, however, would be an improvement.

Ms. MOON. That's undoubtedly true.

Mr. SAWYER. Yes?

Dr. BULGER. One comment that might help here is that since we've released our report out I've been getting questioned, and was on a talk show, and someplace in Phoenix for an hour——

Mr. SAWYER. My condolences.

Dr. BULGER [continuing]. Lots of questions. And, it was interesting that all the questions related to the medical record, and it was very hard to get people to understand that their record is protected and that what is being shared are certain data that are usually not person identifiable.

When this is understood, medical record based research isn't so threatening. I really think that when we collectively deal with public education and the anxiety and paranoia surrounding this research, we really need to separate access to individual medical records per se and access to data abstracted from those records, even if these data are marginally person identifiable.

Mr. SAWYER. You are talking about exactly the question that I'm leading to. It is, how do we begin to reconcile the legitimate public concerns on the one hand and the fears that may be over blown about what access may mean on the one hand, and what I suspect is a profound over-confidence in the level of confidentiality that they perceive existing in the system today.

In virtually every aspect of this debate, on the broader issues of health care reform, I hear people saying, oh, no, we can't do that because if, in fact, we do that then all of this will be jeopardized. And, what they are talking about are circumstances that are a part of their lives today, the question about whether people have enough choice of a physician, for example. They perceive that they have far greater choice than, in fact, their benefits manager at the place of their employment truly offers them. And, yet, those are legitimate concerns.

The concerns about confidentiality, grounded in their physician's oath, and all the rest, really doesn't recognize the broader range of openings in an information system that already exists today. How do we deal with those kinds of questions?

Ms. MOON. One way you do it is keep your eyes on the prize. You have to make it very clear to people the benefits of a national database, and to make it very clear that that kind of database is most useful because it is looking at large numbers of people who

are not identifiable. Make the point that you don't need to identify specific people in order to have a useful database that provides a good sense of what's going on in health care.

And, I think that most people, while they would find some aspects of this frightening, I think it's not too hard to convince them of the worth of some of the very broad analysis that could be done with this, and I think that that's one of the things to emphasize to people.

Mr. SAWYER. Doctor Bulger, would you agree with that, from the experience you just described, that it's easy to assure them of the value of this sort of thing?

Dr. BULGER. Well, it may not be easy, but I think it's——

Mr. SAWYER. But, it's worthwhile.

Dr. BULGER [continuing]. Worthwhile. And, I also think that what you are doing is important. I mean, I think we all feel a little at risk, I do, until somebody makes some sense out of this mess that's out there.

If proper legislation is written and public education is undertaken, we might really be able to do something with it.

I think the other thing that we sometimes fail to acknowledge is the anxiety associated with privacy in publicly funded health care systems like Medicare. What is the incidence of disastrous invasion of privacy that occur in this context?

I can't think of one. I mean, there's lots of fraud, and there's lots of other stuff that goes on, but I guess I'm not tuned into it. I think that, as part of our educational process, we should keep our eyes on the prize, but also focus on where the problems have been.

The large data sets may be tremendously useful and don't have to be serious targets for misuse, if we build proper safeguards around them.

Mr. JUSTER. I think it's easy to overstate the fear, and the concern and the apparent resistance. I think there are, you know, a small number of people that are just very reluctant, very distrustful of government and of everything else, very reluctant to provide any information, and they are basically non-participants. But, that's not characteristic of the great bulk of the population.

The best illustration I can give you is, in a recent survey where we tried to do a merge of very sensitive Social Security earnings records, which are clearly tax records, they were described as tax records in the consent statement, we got 75 percent of a random sample of American households to agree to let us access their records. And, of the 25 percent that wouldn't, I'll bet by the time another two years has rolled around, and we pick up half of those at the second shot to go and agree to have those records.

Now, that's not 100 percent, but I think the point is, most people really don't have this kind of concern. There are people that feel very strongly and very vigorously, and they are quite vocal about it, and we may overestimate the depth of that concern, as opposed to it's a very deep concern for a small fraction of the population, most of the population, quite frankly, doesn't really care much about it one way or the other.

Mr. SAWYER. I think you are absolutely correct, but I also recall an experience that I went through four years ago, where a relatively small number of people who expressed exactly that kind of

reluctance with regard to the decennial Census provoked a license that became a virus in the nation, not to respond for exactly the same kinds of reasons, and I use that term loosely, that represent the kinds of concerns that we've seen measured here. That license provoked a lower response rate than the one that you describe.

Mr. JUSTER. No, I think that's exactly why getting people to understand what functional separation means, and how it can be enforced, that's really very critical. I mean, people have got to develop some confidence that when they participate in one of these activities that, in fact, it is true that their privacy and confidentiality is maintained and there's legal enforcement of this, there are codes of ethics of this, codes of congressional conduct about this, and people are serious about it.

Mr. SAWYER. And, legal sanctions for their violation.

Mr. JUSTER. Yes, and legal sanctions are there, too.

Mr. SAWYER. Yes.

Mr. JUSTER. And, I think over time if that was actually put in place, people would get to feel pretty comfortable with it.

Right now, you don't have those sanctions.

Mr. SAWYER. That's correct. The concerns are based on a system that exists today.

Mr. JUSTER. Right.

Mr. SAWYER. Thank you all very much. You've been very helpful, and I hope that you'll respond to questions in writing, if they are not too voluminous, as well.

Thank you very much.

Our final witness today is Janlori Goldman, who is the Director of the Privacy and Technology Project of the American Civil Liberties Union.

Thank you for being with us, and thank you for your patience, and the same standards that applied to everybody else with regard to the full context of your message applies to you as well.

STATEMENT OF JANLORI GOLDMAN, DIRECTOR, PRIVACY AND TECHNOLOGY PROJECT, AMERICAN CIVIL LIBERTIES UNION

Ms. GOLDMAN. Thank you, Mr. Chairman. Good afternoon.

Mr. SAWYER. Good afternoon.

Ms. GOLDMAN. And, thank you for inviting me to testify here today on H.R. 3137 and the other privacy issues that are raised by the Act and by health care reform generally.

I wanted to just say at the outset that I very much appreciate the comments here today that you've made about privacy and confidentiality, and your acknowledgement and your sensitivity to the issues. It's very important and I appreciate it.

As we've heard today the focus on health care reform of the last year has provided us with a tremendous opportunity in many areas, but also a responsibility as well. We can't just move forward with health care reform and not be attentive to the privacy and confidentiality needs of the public.

The goals of reform, as we've heard, have tremendous benefits; universal coverage, lowering the cost of health care, administrative simplification, which H.R. 3137 is aimed at, improving quality of care and assisting in research.

But, the means to accomplish these goals all seem to revolve around one proposal, which is to create a national information infrastructure. In H.R. 3137, we have the electronic health information network. Such a system is proposed in the Administration's bill. This network seems to be a necessary way of achieving health care reform goals.

At the ACLU we are not total Luddites. We recognize that technology can be used to enhance privacy, as well as undermine it, and, in fact, in some ways there are technological solutions to privacy concerns that we recognize and that we support. But, we need to be especially mindful here that we use technology in a way to bolster confidentiality protections.

The reason that people are focusing on this network is that we are talking about amassing the most highly personal and sensitive information. Congressman Petri mentioned earlier with the example about the grocery store, there are confidentiality concerns about what we buy, what we eat, but when we are talking about health records we are talking about the most sensitive, most vulnerable information that strikes people in the gut. That's why when we hear talk about health care reform and the President waves the card and we talk about an electronic network, people start to get nervous. They are concerned. They are not sure what to be worried about, but they are worried.

As you said eloquently, and a number of the other witnesses said, if we don't protect people's privacy at the outset, they may be loathe to participate in health care reform. They may not fully participate in the ways that we want and in the ways that would achieve the goals of health care reform more broadly.

One of the flaws in both—in all of the bills that we've seen that deal with health care reform, whether it's 3137 or the Administration's package, is that the bills merely set out principles of privacy. They acknowledge the need to protect the information, and they lay out principles, but then they create some other entity, whether it's a health data panel, or a national data board, to develop more specific regulations and then at some point into the future propose legislation that would then come back to Congress, and at some point maybe be enacted into law.

The lack of enforeable standards is a serious flaw in the current proposals. Everybody that we've heard from today, and people that you've heard testify at other hearings on health care reform, all agree we must have the privacy protections up front. There need to be statutory protections and they need to be built into the proposals.

Security and privacy experts agree, you cannot build a network unless you know what you are building, unless you know what principles you are building into law. Otherwise, you have to come back three years, four years, five years later and retool the hardware and software, redesign the systems. It's not only expensive to do that, but in some situations it may not even be possible.

So, I would urge that in H.R. 3137 and in other health care reform proposals that we build the privacy protections in statutorily, up front.

The current environment, as I'm sure that you know, is that we don't have any comprehensive privacy protection at the federal

level for medical records. We have this extremely strong law for video rental lists, thanks to Robert Bork, but we don't have anything for health records. In a Harris survey that was taken last year with the support of Equifax, we found that people live under the mistaken belief that we have comprehensive protection for health records. When they find out that we don't, 85 percent, support the need for comprehensive protection for information in the health care reform context.

The traditional doctor/patient relationship, which has very, very strong ethical protections for the information, has been eroded and dramatically changed by a shift to third-party relationships. The insurers, for instance, do not have a direct relationship, with patients. In fact, they don't even see the patient as their customer, they view the employer in many situations who is paying for the benefit as the customer, and so, they do not really owe a fiduciary relationship, a trust relationship, to that patient. So, that has really dramatically changed the ethical responsibilities between doctors and patients, with reference to personal information.

Why do we need to protect this information? You said it at the outset. If the public does not trust that the information will be protected, they will not participate in health care reform. They will not participate in any new system. They may, in lacking trust, hold back information, which again would be detrimental to research. They may give inaccurate information, which would also be detrimental to research. They may, as you pointed out, just not participate, as we saw with the 1990 Census. They may decide to pay for certain benefits out of their own pocket, if they are allowed to do so under whatever reform proposal becomes law.

Without privacy protections, health care reform will fail. The consequences from unauthorized disclosure are fairly severe. They can be loss of job, embarrassment, damage to reputation, stigma. Fifty million people in the Harris survey said that they believed that they were victims of unauthorized disclosures of health information. Even those who are strong privacy advocates were stunned at that number.

When we talk about consequences, let me give you a very, very real example. During last year's political race for the House of Representatives, Congresswoman Nydia Velazquez, had her medical record from a hospital in New York was faxed to a local reporter. She was devastated. This is information that she had not disclosed to her family, that she believed was absolutely confidential. She sought treatment believing it would be treated as confidential. When the information was faxed, she had to then hold a press conference, discuss these extremely intimate and devastating details of her private life. She won, which I think is a remarkable testament to the American public's ability to get information like that and understand it, and not hold it against her. It may have even made her a more sympathetic candidate.

But she, after a great deal of soul searching, testified a few months ago at a Senate judiciary hearing on the protection of health information. She was the lead witness and talked about the need to have an strong federal law protecting this information.

So, there are very real consequences. Some of the disclosures we never know about. Some individuals may never even know that

there was an improper disclosure. They may not know that the harm to them came from an unauthorized disclosure. It's very, very hard to measure.

So, the solution is to have a comprehensive privacy law to protect health information. There is extremely strong support for this. In fact, I would even go so far as to say that there's a consensus. The American Medical Association has testified in support of a strong law, as has the American Hospital Association, the American Health Information Management Association. There have been a number of reports issued recently supporting the need for federal legislation and the National Academy of Science's Institute of Medicine report referred to here earlier, the Office of Technology Assessment, Congressman Stark has talked about the need to have it be an integral part of reform, as has Senator Leahy. There's work on a bill that Gary Condit is planning to introduce and we look forward to its introduction.

I would urge that this committee, especially considering the sensitivity to the privacy issue that you have, work together with these other members and see if we can do something that takes care of the concerns of the research community and the need to simplify in terms of the administrative world, and also protect privacy together. These are not mutually exclusive goals, and we need to put them in one package.

Thank you.

Mr. SAWYER. Thank you very much.

[The prepared statement of Ms. Goldman follows:]

PREPARED STATEMENT OF JANLORI GOLDMAN, DIRECTOR, PRIVACY AND TECHNOLOGY PROJECT, AMERICAN CIVIL LIBERTIES UNION

Chairman Sawyer and Members of the Subcommittee:

I. OVERVIEW

I very much appreciate the opportunity to testify before you today on behalf of the American Civil Liberties Union (ACLU). The ACLU is a private, non-profit organization of over 275,000 members, dedicated to the preservation of the Bill of Rights. The ACLU's Privacy and Technology Project was established in 1984 to evaluate the impact of new technologies on individual privacy. Over the years, the Project has worked to develop strong privacy policy in numerous areas, including credit reporting, electronic communications, video rental lists, and criminal justice information systems.

The Project's primary goal for the 103rd Congress is the passage of federal legislation that establishes enforceable privacy protection for personal health information. We believe that the need for such legislation is the most critical privacy issue facing this country today. The absence of a strong federal law to protect peoples' health records is troubling. In fact, a recent Louis Harris survey found that most people live under the mistaken belief that their health records are protected by the law. As the country begins debate on reforming the health care system, protecting the privacy of people's health records must be at the heart of any health care reform plan. Such legislation is needed even in the absence of comprehensive health care reform.

The societal impact of technological innovations -- including those that allow personal health information to be transferred easily over great distances -- is staggering. The development of a national information infrastructure and the information superhighway are changing the ways we deal with each other. While the information revolution holds great promise for enhancing our ability to communicate with each other, new technologies must operate within enforceable privacy rules. Eventually, the collection and use of personal health information will take place in an electronically networked environment. Few relationships in the health care field will remain unaffected.

Our statement today outlines the imminent need for federal legislation that creates an enforceable privacy right in personal health records, the public's support for such a measure, and our comments on H.R. 3137, the Health Care Information Modernization and Security Act of 1993. We conclude with our recommendations for the essential privacy protection components to be included in any health information system.

II. HEALTH CARE REFORM AND PERSONAL HEALTH INFORMATION

Recent proposals to reform this country's health care system rely heavily on the automation and linkage of personal health information as a means to reduce costs, improve efficiency and quality of care, and extend universal coverage. The ACLU acknowledges these important

goals, but we urge that they not be achieved at the expense of peoples' privacy.

H.R. 3137 requires that an electronic health care information network be established to achieve these purposes.[1] H.R. 3137 does address the need to protect the confidentiality of computerized personal health information, but, we believe it does so inadequately. Under the bill, a Health Care Data panel is charged with developing proposed privacy regulations, which then must be approved by OMB. The Administration's bill takes a similar approach. All of the responsibility for developing privacy standards and a legislative blueprint is delegated to a National Health Board.

Both bills lack a detailed legislative proposal to accomplish their privacy goals. We do not believe that a health information system can be implemented without statutory privacy policy in place from the outset. It is very difficult, if not impossible, to build privacy and security protections into a system once it is already in place. Privacy and security rules must be the guide that shape the creation of health information systems. Such an amassing of the most sensitive, personal information will seriously jeopardize peoples' privacy if legal requirements are not in place up-front.

---

[1] The Administration's Health Security Act would require the creation of an "electronic data network consisting of regional centers that collect, compile and transmit" biographical and health information on virtually every American (Sec. 5103).

A serious flaw in both the Administration's bill and H.R. 3137 is that the law would apply only to personal health information in computerized form. The privacy principles in these proposals would not apply to paper records. Health care records, in both paper and electronic form, are deserving of privacy protection. The harm that could result to an individual from an authorized disclosure is the same, regardless of whether the health information is on a piece of paper or in a computer. While we recognize that the vulnerability of information to unauthorized use grows as the computer makes possible the instant sharing of information, legislation that only covers electronic information would create a huge loophole - in essence one could avoid the scope of the law by using paper records or making verbal disclosures.

III. THE NEED FOR COMPREHENSIVE FEDERAL PRIVACY PROTECTION

There is widespread agreement among privacy and security experts that protections on information must be built in on the front-end; it is too difficult and risky to try to add them once a system is already in place. Privacy and security must be viewed as the foundation on which health information networks are created. Health care reform is more vulnerable to failure if the public is aware that their health information is unprotected. Americans must have confidence that their personal health information will be safeguarded before they will fully and willingly participate in a new system.

Currently, at the state and local level, employers, insurers, and health care providers are forming coalitions to develop automated and linked health care systems containing lifetime health histories on millions of Americans. Again, the goals are cost reduction and improved quality of care. The scope and strength of health information privacy laws vary widely from state to state. The absence of a uniform federal law to protect the privacy and security of health care information will lead to conflict among the states and cause a setback for the overall goals of privacy protection.

IV. PUBLIC DEMAND FOR PRIVACY PROTECTION

A consensus is emerging that federal legislation is needed to protect the privacy of personal health care records. At a conference in Washington, D.C. this past November co-sponsored by the U.S. Office of Consumer Affairs, the American Health Information Management Association, and Equifax, nearly every panelist and member of Congress supported the need to make privacy an integral part of health care reform. In agreement were panelists from the American Medical Association, CIGNA Health Care, the U.S. Public Interest Research Group, Computer Professionals for Social Responsibility and IBM.

At the conference, Louis Harris and Associates released their Health Information Privacy Survey, prepared with the assistance of Dr. Alan Westin, of Columbia University. The survey found that the majority of the public (56%) favor the enactment of strong

comprehensive federal legislation governing the privacy of health care information. In fact, eighty-five percent say that protecting the confidentiality of medical records is absolutely essential or very important in national health care reform. Specifically, most people want penalties imposed for unauthorized disclosure of medical records (96%), guaranteed access to their own records (96%), and rules regulating third-party access. In addition, most people support the need for an independent, neutral Board to issue regulations and enforce standards on privacy matters (86%).

More broadly, the Harris survey found that a large majority of Americans (80%) are concerned or very concerned about threats to their privacy. A 1992 Harris survey showed that while a large majority of people recognize the benefits to society of innovative technology, nearly nine out of ten people also believe that computers make it easier for someone to improperly obtain confidential personal information. As a result, over two-thirds of the public support tough restrictions on the use of computers.

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. As the most recent Harris survey reveals, individuals are highly suspicious of large scale computerization and believe their medical records are in dire need of privacy protection. 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.

The unauthorized disclosure of personal health information can have disastrous consequences. New York Congresswoman Nydia Velazquez won her House seat only after overcoming the results of an unauthorized disclosure. Her medical records -- including details of a bout with depression and suicide attempt -- were faxed to a New York newspaper and television station during her campaign. In another case, a journalist disguised himself as a doctor, obtained an actress' medical record and published that she had been treated for a sexually transmitted disease.

More commonplace -- and in some ways more troubling than the well-publicized privacy invasions of political figures -- are the consequences suffered by ordinary individuals whose privacy has been compromised by the disclosure of medical information. The 1993 Harris survey found that nearly 50 million people have experienced the unauthorized disclosure of medical information. In one instance, a physician at a large New York City medical school logged on to a computer system, discovered that a nurse was pregnant, and proceeded to publicize that information. And, in Colorado, a medical student sold medical records to attorneys practicing malpractice law. Undoubtedly there are millions of similar breaches that occur without peoples' knowledge. Further, errors in peoples' medical records have been difficult for them to correct and control.

Despite the horror stories -- both public and private -- many Americans believe that the information they share with their doctor is kept private. The traditional nature of the doctor-patient relationship is intended to foster trust and to encourage full disclosure. However, once the patient's information is submitted to a third-party payor, or to any other entity, the ethical tie between doctor and patient evaporates. In fact, in a particularly telling statistic, 93% of those termed "leaders" in the Harris survey, including hospital CEOs, health insurance CEOs, physicians, nurses, and state regulators, believe that third party payors need to have detailed confidentiality and privacy policies.

Within our current health care system, people are trying to protect themselves against potential privacy violations. Some people routinely ask doctors to write down a false diagnosis because they fear their employer may see their records, or some people don't even tell their doctors everything about their condition for fear of losing control over sensitive information. In psychiatric practices, it is common for patients to ask their doctors not to take notes during sessions out of fear they could be leaked or even obtained legally with a subpoena. Also, some people try to avoid the creation of a record altogether by paying for medical services out of their pockets, even though they are entitled to insurance coverage.

In the end, any system that fails to win the public's trust will fail to win the public's support. Once the public recognizes that

their right to control information about themselves within a health information system is weak, they will withdraw from full and honest participation. We should not allow individuals to fall through the cracks because their privacy is not protected, or make the loss of privacy the necessary price for the receipt of health care. People should not be forced to give up their privacy and their right to control information about themselves as the cost of participation in society.

V. CONGRESSIONAL ACTION

A great deal of attention is being focused on establishing a national privacy law to protect personal health records. In November 1993, the House Subcommittee on Government Information, Justice and Agriculture of the Committee on Government Operations held a hearing on the confidentiality of health care records. That Subcommittee, chaired by Gary Condit (D-CA), has just completed drafting a comprehensive health information privacy bill. We look forward to the bill's introduction. The Senate Judiciary Subcommittee on Technology and the Law held a hearing on January 27, 1994 to address confidentiality and health care reform. The chair of that subcommittee, Patrick Leahy (D-VT) has expressed his commitment to ensuring that health care reform proposal embody strong privacy safeguards.

Further, the Office of Technology Assessment (OTA) recently

issued a report entitled "Protecting Privacy in Computerized Medical Information," which addresses the effects of the computerization of medical records on peoples' privacy. In recommending comprehensive federal legislation, OTA found that:

> (t)he expanded use of medical records for nontreatment purposes exacerbates the shortcomings of existing legal schemes to protect privacy in patient information. The law must address the increase in the flow of data outward from the medical care relationship by both addressing the question of appropriate access to data and providing redress to those that have been wronged by privacy coalitions. Lack of such guidelines, and failure to make them enforceable, could affect the quality and integrity of the medical record itself. (OTA Report, p. 44).

Also, the National Academy of Science's Institute of Medicine (IOM) just released a study that focused on the risks and opportunities associated with protecting the privacy and confidentiality of personally-identifiable health data in regional data centers. The IOM report recommends that the U.S. Congress enact preemptive legislation that will "establish a uniform requirement for the assurance of confidentiality and protection of privacy rights for personally-identifiable health data and specify a Code of Fair Health Information Practices that ensures a proper balance among required disclosures, use of data, and patient privacy" (Recommendation 4.1). The IOM also recommended that a responsible administrative unit or board be established. In addition, the Department of Health and Human Services' Task Force on the Privacy of Private Sector Records sponsored a conference last year on the confidentiality of health records. All of these efforts represent a tremendous pulling together

of the public and private sector to achieve a critical goal -- the passage of a health records privacy law.

Over fifteen years ago, there was similar pressure to craft such a privacy law. In 1977, the federal Privacy Protection Study Commission issued a report recommending legislation to protect private sector records, including medical and insurance records. The Commission's recommendations sparked the only other Congressional effort to enact a medical records privacy bill. In 1980, due in part to pressure from the law enforcement community for unfettered access to health records, the legislative effort failed.

Today, 15 years after its first efforts, Congress has both the opportunity and responsibility to seize this chance created by the current focus on health care reform and enact comprehensive legislation protecting the privacy of health care information. We urge that this Subcommittee support a comprehensive privacy protection bill, as part of H.R. 3137 or as part of a national health reform plan.

V. RECOMMENDATIONS

The following are our recommendations for the key provisions we believe should be included in a federal health records privacy law:

1) Personally-identifiable health records must be in the

control of the individual. Personal information should only be disclosed with the knowing, meaningful consent of the individual;

2) Limits on access and disclosure should apply to all personally identifiable health data regardless of whether the information is in paper or electronic form;

3) Information that is not personally-identifiable may be provided for research and statistical purposes;

4) Health record information systems must be required to build-in security measures to protect personal information against both unauthorized access and disclosure from within;

5) Employers should be denied access to personally-identifiable health records on its employees or prospective employees;

6) Individuals must have the right to see, copy and correct all information contained in their records;

7) Individuals should be given notice of how personal information will be used and by whom;

8) Both a private right of action and a government enforcement mechanism should be established. A federal oversight

process should be put in place to be conducted by a National Health Board or Data Protection Board;

9) If a card is created, such as the Administration's Health Security Card, it should be used only for identification purposes and be limited to the health care context. Any other uses, such as by law enforcement or employers, should be strictly prohibited.

CONCLUSION

The ACLU believes that the protection of personal health information must be central to all health care reform proposals. Even in the absence of health care reform, we believe that a comprehensive, enforceable privacy law is necessary. We commend this subcommittee for recognizing the need to protect privacy in H.R. 3137. We urge that a legislative privacy proposal be developed prior to the creation of an electronic data network.

There is no more pressing privacy issue than the protection of peoples' health care records. With health care reform one of the top political priorities, we have an opportunity and a responsibility to make privacy an integral component of any new plan. We have come a great distance in achieving a broad consensus on the key principles. The more difficult task ahead will be to reach agreement on the details. We look forward to working with you on this endeavor.

Mr. SAWYER. I want to assure you that we are not only aware of the work that's going on, we've attempted to craft a piece of legislation here that will fit, much like a battery, a wiring system, and can be moved from automobile to automobile, but is central to the operation of that system. We are trying to build a system that will accomplish the kinds of goals that you and others have described, and that will actually be compatible with each of the larger health care reform proposals, because, frankly, some of them simply will not work without this kind of information system.

And, at the same time, we want to work with Representative Condit and his Subcommittee on the Government Operations Committee, to make sure that the legislation that he crafts fits hand and glove with the work that we are doing here. Only in that way will the two in combination be able to fit into a wide variety of potential overall reform proposals.

Let me ask you a question that I've asked others, and I hope you'll understand that I don't mean it as a simplistic question. It is really one of the more difficult questions, I think, in all of this. It's a question that I'm not sure is resolved in today's society, but one that we need to resolve if this is going to work to the level of expectation that you've articulated here today. That is, who owns the records, who owns the identifiable data, and then, perhaps, subsequently who becomes the responsible custodian for those data? It may not be the individual.

And, certainly, as those data becomes masked, separated and available for use for broader public purpose, who ought to be responsible for those data as they are used?

Ms. GOLDMAN. Well, I think as Nan Hunter said earlier, the question of who owns personal information is a very complicated legal question. What I'll try to do is answer it more from a policy standpoint.

I believe that people own information about themselves, that information about themselves reflects who they are, how they want to be perceived, what they want others to know about them, and that without the control over that information they have lost their right to privacy.

I don't believe that that control should be absolute, however. I don't think that any right to privacy, no matter what you are talking about, is absolute. In fact, we are always balancing privacy against other societal needs, but I think as a starting point we need to view the information about people as a part of them, and, therefore, something that they should maintain some decision-making control over.

So, at the point at which they give information over, whether it's to a doctor, to a payer, to an employer, they should be able to say, I'm giving you this information for one purpose, but I don't want it used for any other purpose without my consent. I'm consenting to this particular use but not other unintended or secondary uses.

And, I think in that sense then, the person who is receiving the information may also have some rights in the information. They may also, in some senses, own the information, but that doesn't give them the right to do anything with it that they please.

And, I think certainly in the health area, we want people to give information. There are extremely good uses and benefits to be

gained from people giving information, but in order to encourage full participation and full disclosure you have got to have the protection, you've got to have that protection between the two individuals as against third parties who may want access to it. Otherwise, I think people will not fully disclose, and so there's a real benefit here towards having an ownership and a control in the information that the individual has.

Mr. SAWYER. Do you agree with the notion that we've heard described here and elsewhere of functional separation, is it sufficient to draw that great wall of China between the functions, and, if so, how do you see the governance of those two functions, and, particularly, at the point where there are decisions that have to be made about interaction between the two?

Ms. GOLDMAN. Well, I think that separation, as we've heard described here today, would go a long way towards protecting the privacy of individuals. For instance, we acknowledge that there's a need to disclose information for payment purposes, for certain research purposes, that in any situation where you can get the individual's consent, obviously, that is the way to go, but that in terms of a separation I think that it's useful, but is not—again, it is not an absolute protection, that there's no guarantee that in having the separation, the functional separation, that you are then going to protect privacy. I don't see it as kind of the great safeguard maybe that others do.

Mr. SAWYER. I keep asking the question about whether the governance of those two sides of the wall ought to be by a single entity that makes decisions about which way it tips, or by two entities in tension with one another, with competing mandates, one to protect and one to make responsibly accessible.

Ms. GOLDMAN. Well, the entities, I mean, I think everybody's health care reform proposal creates some kind of an entity, some kind of umbrella entity that will make all kinds of decisions, issue regulations and guidance, and propose statutory language, and most people envision that the entities will be made up of a diverse group of people.

And, again, while I think that that's helpful, and it's something far better than what we have today, we don't have anything in the privacy world that looks exactly—that looks anything like that.

There have been in other instances, there's, I think, Congresswoman Cardiss Collins and Senator Simon have both introduced bills that would create a data protection board to look broadly at data protection issues throughout the public and private sector, to try to relieve some of these existing tensions, and the National Health Board would do something more specifically in health. But, I think that that would certainly be useful, because, again, we don't want to leave—my worry is leaving the decision-making authority to the person holding the record. I think that once you've got the information, once you have an interest in using it, it's going to be very hard for you to step away and make any kind of an objective judgment as to whether the information should be protected or safeguarded.

Mr. SAWYER. One of the toughest battles in all of this is the one that we've been talking about with each of the panels. It is the question of public understanding of the weaknesses in the system

that we now have, and the importance of both establishing high standards for what we try to build on the one hand, and understanding that this is not at its best to jeopardize what exists today, but to be a very substantial improvement.

This is the point that you made about technology offering promise of greater protection than we've ever seen before, as opposed to the risk of dissemination.

Would you talk a little bit about that public education function and how we best go about that?

Ms. GOLDMAN. I think the public education function here is huge. In fact, I would go so far as to say it's overwhelming. I just heard yesterday, people are having a hard time understanding the details of health care reform, let alone understanding whether or not their health information will be protected.

If there is a card created, which we've heard a lot of talk about a card, I think it will bring home to people that this card is being used as the means to link information in other databases. I think it will make it clear to them in a way that it isn't clear today to many people, that we have a national network, that we have a system that allows for the immediate exchange and manipulation, if you will, of the information. So, I think people will understand it much more clearly.

And, in terms of public education, privacy has got to be the first thing out of the mouths of both the government officials and those in the private sector who are trying to sell this plan. I think we've seen a tremendous increase in the attention of the Administration over the last few months to this issue, as after their proposal came out it was clear that their bill embodied privacy principles but, again, not statutory language, and there was a great deal of concern about that from members of Congress and members of the public.

So, I think that the public education campaign has to start at the very top. The President and members of the Health Care Task Force and members of the Administration have got to talk about privacy being an integral component of health care reform, and that we will do a better job to protect privacy than we are doing in our current environment, that this is an opportunity, again, to enhance the protections.

I mean, I would just say that that should be one of the first selling points, if you will, of the legislation.

I think that one of the easiest public education opportunities is at the point of service, the initial contact between the patient and the provider, or the patient and the employer, the employee and the employer, in terms of saying this is how information about you will be collected, this is how it's going to be used, these are your rights, these are our responsibilities and allowing people to know right at the front end what the protections are, because if everyone is going to have to enroll this is a wonderful opportunity to inform them of their rights, if they have them. And, again, I'm saying that I think that they must have them.

Mr. SAWYER. It can't be something to be developed later.

Ms. GOLDMAN. Absolutely not. I think the danger is—

Mr. SAWYER. That's one of the reasons I'm really concerned about the time lines involved in all of this. It is not just an idle mistrust

of the time lines that you place in an enactment schedule that may or not be achieved. It is the concern that we cannot put all of this in place without having some of these things first, and this, as you suggest, is primary in any set of enactments.

Just a final question. One of the great hopes that many of us who are concerned more broadly with national statistical systems involves the use of administrative information. I don't mean identifiable information, but the way in which we measure ourselves as a people. There's a growing hope that administrative records can help us achieve, perhaps, an even greater statistical accuracy, and certainly a greater timeliness in terms of many, many of the different things that we measure about ourselves.

You've heard real discussion about the importance of timeliness with regard to the medical data and broad public policy. Could you react to the importance of being able to share administrative records in a way that serves those goals, the kinds of protections that those represent, and the interaction of federal statistical agencies?

Ms. GOLDMAN. As long as information which is disclosed is not personally identifiable we don't have any concern with the disclosure. And, I use the term "personally identifiable," which you see in the IOM report, and you see in many other areas, to mean, as I think an earlier witness said, no, we're not just talking about name, address and Social Security number, but if the information in the record can reveal the identity of the individual it should not be disclosed in that form.

And, I think the Census Bureau, for instance, is extremely sensitive to this. They mask data, they scramble data, so that in a small block, for instance, where there are certain salient facts about an individual that would allow you to identify that person, they mask it, or change it, or do something with it, and I would urge that that be done in this context as well.

Also, there's been some talk about providing information to the Census from the electronic data network established here. I would have very serious misgivings about that. There was a hearing a number of years ago in the Senate about supplementing the Census with information compiled by other agencies, and the privacy concerns there are real. The Privacy Act, for instance, prohibits sharing of information between agencies, personal information between agencies, and I think we need to be very careful, again, partly because of the public's trust, and how things will be perceived, but I think there is a real privacy concern about sharing the information that's given for one limited purpose, which is health delivery.

Mr. SAWYER. But, the distinction that you are making is with regard to personally identifiable data.

Ms. GOLDMAN. Absolutely. All other information, I don't think the ACLU would have any concern about, as long as you cannot pinpoint the individual. We think it should be released. There are tremendous benefits there.

Mr. SAWYER. Let me ask you this, because I expect to hear about it from others. The ability to use enormous amounts of transactional information, and the ability to disaggregate that, using very powerful data sorting techniques, it is a risk, it is, perhaps,

a remote risk, you are not talking about that kind of potential, I assume. I mean, there is no masking system ultimately that you or I could guarantee to be perfect.

Ms. GOLDMAN. You can't guarantee, and, in fact, I appreciate you raised that point. We have said over and over that while we recognize the tremendous benefits here, that there will always be a risk once the electronic data network is in place, I don't care how many fire walls we build around it today, tomorrow there will be a reason to erode them and Congress will rubber stamp that.

Mr. SAWYER. Well, no, I'm not talking about reasons to erode, but I'm talking about techniques to get around.

Ms. GOLDMAN. Yes.

Mr. SAWYER. Because I think we can hold a representative government responsible for those kinds of decisions. The Census has been held sacrosanct for many years, that doesn't mean that it's not technically possible given enough will to get around it.

Ms. GOLDMAN. No, I agree, and I think that we've seen it with the Census, we've seen how the private sector has used Census tract data with extremely sophisticated information technology and information from other databases, they have been able to feed it all in.

Mr. SAWYER. But, that wall has never been breached.

Ms. GOLDMAN. That's right.

Mr. SAWYER. Yes.

Ms. GOLDMAN. Well, there were two earlier breaches, but they were very early, they were before 1945. There haven't been any recent breaches.

But, I think that we have to, as a society, accept that there will be risks. There will be risk of breaches, even if, you know, we are optimistic that the protections will be sacrosanct, and I think we also have to realize that there will be a tremendous pressure to use the information in the private sector for commercial purposes, and that even with the information that we would consider non-personally identifiable at the outset, there will be ways, there will always be ways to try to pinpoint individuals by using information from other databases.

Mr. SAWYER. But, that's not what you are talking about in making these distinctions here.

Ms. GOLDMAN. Right.

Mr. SAWYER. I'm grateful for that.

I think one of my real concerns in all of this has been, I have great confidence that we have the capacity to develop a very good system. We have the will to do it. My concern has always been that because it will not be perfect, undemonstrably, provably perfect, that we will not have the opportunity to develop something that will be a very substantial improvement over what we have today. It is really one of those cases where the perfect does become the enemy of the very good.

Thank you very much for your testimony today. I thank all of our witnesses, and I hope that we'll be able to return to you and your organizations from time to time as we attempt to achieve the goals that you've outlined for us.

Thank you.

Ms. GOLDMAN. Thank you.

Mr. SAWYER. If there's no further business to come before us, we stand adjourned.

[Whereupon, at 1:16 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

JOINT PREPARED STATEMENT OF THE HEALTH INDUSTRY MANUFACTURERS ASSOCIATION AND THE CENTER FOR HEALTH INFORMATION MANAGEMENT

The Health Industry Manufacturers Association (HIMA) and the Center for Health Information Management (CHIM) have chosen to speak with one voice in addressing the provisions of administrative simplification in any health reform legislation. Both HIMA and CHIM enthusiastically support efforts to simplify and automate the administrative aspects of health care delivery and financing. HIMA is a national trade association of more than 700 companies representing manufacturers of medical devices, diagnostic products, and health care information systems (HIS). CHIM is also a national trade association representing 57 manufacturers, consultants, and telecommunications firms in information technology. The manufacturers of information technology in health care provide systems and services for financial processing, management functions, and clinical care. It is through these companies that HIMA and CHIM are able to share with the Subcommittee the experience and insight gained from developing, integrating, and supporting computer software for hospitals and physician offices across the country.

The administrative simplification reforms being considered by the Subcommittee primarily concern methods for improved use of clinical data. This underscores the critical fact that *health care is an information industry* -- most health care providers spend the majority of their time creating or using information. Significantly, only a small percentage is then abstracted and submitted to payers, reviewers, and other agencies. The rest is maintained on paper at high cost and is not readily available for review or analysis. Although it is an information industry, health care lags behind almost every other information industry in its level of investment in information support, and in its use of automation to improve efficiency, effectiveness, and quality.

We look forward to continuing to participate in the development of broad scale administrative simplification methods for the health care systems of the future. Whatever path is chosen in this reform process for providers, payers, and patients, it is the information industry who will be tasked with making it work.

Summary

The following statement describes the quality enhancement and the cost savings of the clinical HIS applications, as well as recommendations for further improvement in the use of information technology in health care. *Most significantly, we recommend the rapid development of standards, for both data requirements and electronic transmissions. Additionally, we strongly recommend the use of the computer-based patient record.* HIMA and CHIM believe that this effort can improve appropriate access to health information, improve data quality and availability on a national level, and most importantly improve the quality of patient care. Ultimately, it will provide the necessary data for health care reform and assessment of the health care system. While HIMA's and CHIM's HIS companies develop both financial and clinical HIS applications, the following statement will focus on the clinical applications.

SYSTEM CAPABILITIES
Clinical Applications

Financial processing already involves provider time to some extent. The administrative portion of clinical care requires an even greater investment of time. About one-third of a physician's time and almost one-half of a nurse's time is spent doing clerical/administrative work; time that could be far more effectively invested in patient care. There is a belief among some that systems to provide clinical management improvements are years away. In fact, the kinds of applications necessary to improve clinical efficiency and the quality of our health care system exist now and are in operation in selected areas. For instance:

- New York University Medical Center was the first hospital in the U.S. -- and possibly the world -- to mandate 100% direct physician utilization of its clinical information system for order entry. Now, more than 10 years later, over 10,000 physicians and nurses have been trained on the system and it is considered an essential tool to improve care delivery, meet stringent New York documentation and other state regulations and capture thousands of dollars in what would have otherwise been lost revenue. Citing only one area of care-delivery improvement, NYU officials have noted that the medical center administers 10,000 medication doses in an average 24-hour period. While the generally accepted norm for serious medication errors is approximately 1 percent (which for NYU would be 100 *per day*), the medical center only experiences about 1 to 2 such errors *per month*.

- North Mississippi Health Services is a growing, diversified regional health care services provider, bringing services to residents in a 60-mile radius of mainly rural Mississippi. The Tupelo-based NMHS includes a 647-bed medical center, community hospitals, nursing homes, a multi-site home health agency, numerous specialty clinics, an HMO, and a growing number of physician office practices. The organization has brought its patient-care information system into virtually all aspects of its organization and has over 80% of its medical record automated, including nurses notes, care plans automated discharge summaries and much more. Hospital officials state that the information system, "is the glue that holds our entire health care system together. Information access is the key to providing cost-effective care in a managed-care, capitated environment."

- At the Graduate Health Care System in the Philadelphia area, four hospitals and several hundred physicians are continuously on-line to an integrated lifetime patient record. This means that when patients are admitted to any hospital in the Graduate system, or are seen by any area physician with privileges, all patient information is immediately available. This dramatically simplifies care management and charting in both hospitals and physicians' offices. In some departments, workloads have increased as much as 33% without additional staffing.

- The New York City Health and Hospitals Corporation, the largest non-Federal public health care provider in the country provides integrated care in 11 hospitals (10,500 beds), five long term care facilities, and numerous outpatient clinics. The

Corporation is installing an automated patient care system. In its evaluation, the Mayor's Private Sector Survey determined that the HIS system is designed to provide a lifetime clinical record with access from anywhere in the city, and provide for *complete payback in six months.*

Benefits of Clinical Applications

In summary, state-of-the-art hardware and software already available from HIS companies can significantly decrease the amount of time health professionals must spend delivering "paper care" instead of patient care. A study by Arthur D. Little has determined that appropriate automation of clinical information alone could save $30 billion. These systems save money, improve the quality of care, and facilitate review and research.

On-line integrated patient-centered-systems assure that the proper information necessary for making both clinical and administrative determinations about a patient's status is collected as it becomes available and delivered when and where it is needed. Otherwise, the information is managed in separate steps after the event, a process which introduces significant costs and exposure to error. Explicit benefits emerge from such applications. Examples include:

- Point-of-care based automation allows appropriate screening of data to be performed as care is being given, whether it be at the bedside, in the examining room, or in a physician's office. Because data is captured in real time, it can be checked for appropriateness, completeness, and errors as care is delivered.

- Detecting potential problems as they occur enhances quality and reduces the need for additional administrative staff who now attempt to detect such problems retrospectively.

- Because of the clerical burden in the delivery of patient care, most integrated patient-centered systems have been shown to save from one-half hour to one and one-half hours per provider per shift when properly implemented. Because 60-80% of health care operating costs are personnel costs, this amount of time saving can provide a significant level of cost reduction.

- Purchasers of such systems have typically experienced a payback on the investment in two to three years with a seven-year useful life of the equipment. Larger users have even faster returns on their investments.

More importantly, as savings are achieved, the quality of the data actually improves. In practice, the elimination of paper documentation and control systems improve data quality by amounts as high as 40%. The increase in data quality is experienced for all forms of data processing -- clinical, financial, and administrative.

Finally, the automation of the bulk of the clinical record allows the extraction of information necessary to perform medical care appropriateness and reasonableness oversight. It also

supports the kind of medical effectiveness research currently being undertaken by the Agency for Health Care Policy and Research and others. With the on-line availability of most or all clinical and financial data, quality assurance and utilization review activities can be performed at central sites in an automated fashion, rather than on a case-by-case basis using expensive chart reviewers. As practice parameters, case management, care maps, and other concurrent control mechanisms are put into place the required amount of monitoring staff would usually increase. However, the ability to monitor such control mechanisms both within the institution and at payer locations using largely automated techniques will enhance the quality of care, and will significantly increase the quality of the evaluation process while decreasing the cost. Better still, the availability of uniform data as recommended later in the testimony will make such reviews more fair and more reliable.

As an example of the kind of studies that could be conducted with greater speed and reliability, let us consider outcomes research taking place on therapies for prostatic disfunction in men. There are essentially three ways to study such a condition. The typical prospective study would collect data from a small (100-300) sample of patients, then analyze and report on its findings. This method requires a significant investment in time, often recollecting data that might have been available at the time the patient was first seen by his physician. Alternatively, 500 patients might be retrospectively considered such as in projects currently being conducted by the Agency for Health Care Policy and Research. However, the preferred method would be to draw the information from clinical records already being maintained on the universe of prostate patients, improving both the speed of the study and the reliability of the findings. Medicare is already paying for hundreds of thousands of such evaluations, but the results are not as readily available for outcomes analysis.

To be effective, it is important to emphasize, however, that *complete* data be collected at the point of care, not just abstracts -- an abridged summary of the medical record, gathered after the fact -- as some would recommend. Complete, concurrent data is needed to make better policy decisions on a broad scale.

HIMA and CHIM believe the provisions of HR 3137 would greatly expedite the movement toward a more efficient and effective health care delivery system. The key to achieving these goals lies in establishing the uniform use of standardized comprehensive non-abstracted data elements and data sets for both medical records and claims processing.

INCENTIVES FOR RAPID IMPLEMENTATION

Standardized Information

Because HIS companies provide systems that manage clinical and financial data which must be shared with a wide array of interested parties, the question of information standards becomes essential. It is clear that the better and more comprehensive the standards for health care data interchange, the better the integrity of the data reaching payers, reviewers, and researchers. Informatics standards should govern communications regarding a range of activities from claims processing to direct clinical care. Additionally, the standardization and

automation of the bulk of the clinical record allows the rapid extraction of information necessary to perform care appropriateness and reasonableness review, and to support the kind of medical effectiveness research currently underway by the Agency for Health Care Policy and Research and other outcomes oriented groups.

In the health care industry, a number of independent entities need to store and share information (e.g., hospitals, physicians' offices, payers, utilization review agents, and researchers). Many providers have invested in HIS software to store and retrieve data for a variety of purposes. One of the functions that comprehensive HIS software accomplishes is communication with providers of patient care, payers (both public and private), and utilization review agents. Increasingly, those performing outcomes research should also be able to take advantage of these improvements. It is then that the greatest strides in care quality will be realized as providers have more rapid access to the latest information on treatment modalities.

Informatics standards enable efficient communication through electronic data interchange. Standards should specify the discrete items and kinds of information (data elements) that are needed for each type of communication, and format of those data elements. While providers might all have customized computer software from several different companies, informatics standards enable entities to communicate with one another. An information user need not require that providers have a specific HIS software package to achieve these savings whether for patient care or claims management. Hospitals and physicians' offices may purchase *different* HIS systems, but still communicate easily if the information to be exchanged is standardized. Further, research protocols may vary from one study to another, but if the data requirements are standardized, then more comparable information might result.

State lines present another potential stumbling block. If informatics standards are permitted to vary from state to state -- as might occur if a plan is developed that encourages states to experiment with reporting requirements -- providers, and ultimately payers, will incur higher costs to acquire software to meet these varied requirements. Additionally, software for hospital systems that serve patients in more than one state would be significantly more complex and costly. And, the clinical, quality, and cost data for each state will be incompatible for analyses of the efficiency and efficacy of care. Therefore, while payment systems may themselves differ, states or other entities should not be able to request exemptions from using uniform national informatics standards.

The bulk of the efficiencies and savings will not be achieved unless <u>all</u> health care entities conform to uniform national standards. Judging from early analyses of likely health reforms, the vast majority of providers may continue to treat patients covered by a variety of health benefit plans. Without extensive standardized clinical data, the value and quality of such care will be impossible to estimate. Hospitals and physicians are likely to need to communicate with a variety of payers, utilization and quality assessors, and others. If providers continue to be faced with the current incompatible requirements, then they will also continue to spend increasing time and money training staff to manage more complex requirements. *HIMA and CHIM believe that mandating uniform data elements and comprehensive uniform clinical data sets would be one of the simplest mechanisms for*

gaining immediate system-wide improvement in health care information while achieving administrative savings.

The American National Standards Institute (ANSI) has created the Health Care Informatics Standards Planning Panel (HISPP), with extensive participation of providers, payers, and HIS manufacturers, to coordinate the development of informatics standards. HISPP directs an interactive process for all electronic data communications in health care. When similar information must be communicated for more than one purpose, HISPP ensures that the various standards do not impose incompatible formats for that information. If additional standards become a part of the future health system, HIMA and CHIM recommend that HISPP coordinate their development to avoid duplication of effort and incompatibility with existing standards. If standards are developed without such coordination, providers and payers will bear the costs.

Adequate Investment in Information Infrastructure

As noted above, the health care system in the United States devotes considerably less resources to information support than do other information industries. The operational problems generated by this low level of investment are compounded by a far higher level of spending for highly trained health care providers to perform administrative chores that should be automated. Improved availability of capital resources would assist in rectifying this impediment to effective and efficient health care delivery. Incentives which encourage investment in providers' information infrastructure rather than in physical plant would be a significant benefit. Such incentives could be in a number of forms including financial benefits such as adjustments to payment formulas, participation requirements based on on-line availability of standard clinical data and the like.

* * * * *

In conclusion, a wealth of benefits can be derived from the full implementation of health information systems. HIMA and CHIM believe that mandating uniform comprehensive clinical data sets would provide major cost savings, and would greatly facilitate patient care and outcomes research, crucial needs for any reformed system. Better clinical and financial information and rapid access to it will provide improved health care delivery by clinicians, better quality of care for the patients, and greater efficiencies and effectiveness for the aggregate health care system.

Additional savings will come from systems used to determine the adequacy, appropriateness, and sufficiency of services especially those that and do so in real time before additional costs are incurred. These procedures, such as utilization review, quality assurance, and other concurrent and post treatment analyses are a major focus for both providers and payers and are a key to both the cost and the quality of care. Examination of the administrative

overhead invested in accumulating these parameters reveals a large number of additional areas where costs can be reduced or eliminated by the use of clinical systems which can deliver large amounts of standardized clinical data. Importantly, such electronically available clinical information provides the necessary infrastructure for accurate national outcomes assessment.

The U.S. health care system has increasingly found itself a victim of an unwinnable paper chase. Providers and payers both spend a major portion of their time and resources performing administrative tasks which are often duplicative or conflicting. The technology already exists for addressing many of these areas but has for a variety of reasons has not been widely implemented. The health information system companies were among the first to realize the potential benefits of the applications being reviewed by the Subcommittee. We believe that even greater potential will be found as these systems are more broadly examined. HIMA and CHIM members who will provide the systems to effect the savings and other improvements can facilitate the transition to a fully automated system. We would welcome working with the Subcommittee to provide continuing industry information on actual system capabilities.

78-222 (224)

ISBN 0-16-044775-5