CONFIDENTIALITY OF HEALTH INFORMATION

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JULY 20, 1999

Serial 106–29

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
64–128 CC WASHINGTON : 2000

COMMITTEE ON WAYS AND MEANS

BILL ARCHER, Texas, *Chairman*

PHILIP M. CRANE, Illinois
BILL THOMAS, California
E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
AMO HOUGHTON, New York
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
JENNIFER DUNN, Washington
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
PHILIP S. ENGLISH, Pennsylvania
WES WATKINS, Oklahoma
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY HULSHOF, Missouri
SCOTT MCINNIS, Colorado
RON LEWIS, Kentucky
MARK FOLEY, Florida

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ROBERT T. MATSUI, California
WILLIAM J. COYNE, Pennsylvania
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
KAREN L. THURMAN, Florida
LLOYD DOGGETT, Texas

A.L. SINGLETON, *Chief of Staff*
JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON HEALTH

BILL THOMAS, California, *Chairman*

NANCY L. JOHNSON, Connecticut
JIM MCCRERY, Louisiana
PHILIP M. CRANE, Illinois
SAM JOHNSON, Texas
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
PHILIP S. ENGLISH, Pennsylvania

FORTNEY PETE STARK, California
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
JIM MCDERMOTT, Washington
KAREN L. THURMAN, Florida

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

CONFIDENTIALITY OF HEALTH INFORMATION

TUESDAY, JULY 20, 1999

HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON HEALTH,
Washington, DC.

The Subcommittee met, pursuant to call, at 3:20 p.m., in room 1100, Longworth House Office Building, Hon. Bill Thomas (Chairman of the Subcommittee) presiding.

[The advisories announcing the hearing follow:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON HEALTH

FOR IMMEDIATE RELEASE
July 13, 1999
No. HL–8

CONTACT: (202) 225–3943

Thomas Announces Hearing on Confidentiality of Health Information

Congressman Bill Thomas (R–CA), Chairman, Subcommittee on Health of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing on proposals to protect the confidentiality of patients' health care information. The hearing will take place on Tuesday, July 20, 1999, in the main Committee hearing room, 1100 Longworth House Office Building, beginning at 2:00 p.m.

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

BACKGROUND:

Section 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104–191) required the Secretary of Health and Human Services to develop policy recommendations with respect to the confidentiality of health information by August 1997. Specifically, the HIPAA mandate required that this new policy be designed to protect the privacy of personal health information that is transmitted electronically, in conjunction with one of the standardized health transactions established by HIPAA's administrative simplification provisions. Secretary Shalala submitted these recommendations to Congress in September of 1997. Under HIPAA, Congress has until August 21, 1999, to enact a privacy law. If Congress fails to enact a medical privacy law, the Secretary is then required to issue regulations within six months. The law provides that, if regulations are issued, they will not supercede stricter State privacy laws. The Subcommittee began its exploration of this issue with a hearing on March 24, 1998. At that meeting, Subcommittee members heard from a variety of private witnesses, as well as Dr. Don Detmer, then Chairman of the National Committee on Vital Health Statistics (NCHVS). The NCVHS advised the Secretary in the development of her policy recommendations.

In announcing the hearing, Chairman Thomas stated: "The importance of information to America's modern health care delivery system cannot be overstated. The rapid exchange of information B much of it personal in nature B is critical to the delivery of high quality care, the increasingly complex financing of care, and ongoing efforts to improve quality. Protecting the confidentiality and security of this information is even more important. Only by protecting the confidentiality of health information can we give patients the confidence they need to seek help, even for the most personal or sensitive of health issues. Data integrity and system security measures are critical to our ongoing efforts to improve health care outcomes and find new cures through the application of information technology to medical research. Today, every patient B including 38 million Medicare patients B benefits from the extensive use and exchange of information in our health system. However, our laws need to be updated to better protect the confidentiality and security of this information.

FOCUS OF THE HEARING:

The hearing will focus on various aspects of the patient confidentiality issue that have been raised by the Secretary's recommendations to Congress and by other laws . The Subcommittee will receive testimony from several public agency representatives and from a variety of private sector witnesses representing different perspectives from within the health care system.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Any person or organization wishing to submit a written statement for the printed record of the hearing should submit six (6) single-spaced copies of their statement, along with an IBM compatible 3.5-inch diskette in WordPerfect 5.1 format, with their name, address, and hearing date noted on a label, by the close of business, Tuesday, August 3, 1999, to A.L. Singleton, Chief of Staff, Committee on Ways and Means, U.S. House of Representatives, 1102 Longworth House Office Building, Washington, D.C. 20515. If those filing written statements wish to have their statements distributed to the press and interested public at the hearing, they may deliver 200 additional copies for this purpose to the Subcommittee on Health office, room 1136 Longworth House Office Building, by close of business the day before the hearing.

FORMATTING REQUIREMENTS:

Each statement presented for printing to the Committee by a witness, any written statement or exhibit submitted for the printed record or any written comments in response to a request for written comments must conform to the guidelines listed below. Any statement or exhibit not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All statements and any accompanying exhibits for printing must be submitted on an IBM compatible 3.5-inch diskette in WordPerfect 5.1 format, typed in single space and may not exceed a total of 10 pages including attachments. Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. A witness appearing at a public hearing, or submitting a statement for the record of a public hearing, or submitting written comments in response to a published request for comments by the Committee, must include on his statement or submission a list of all clients, persons, or organizations on whose behalf the witness appears.

4. A supplemental sheet must accompany each statement listing the name, company, address, telephone and fax numbers where the witness or the designated representative may be reached. This supplemental sheet will not be included in the printed record.

The above restrictions and limitations apply only to material being submitted for printing. Statements and exhibits or supplementary material submitted solely for distribution to the Members, the press and the public during the course of a public hearing may be submitted in other forms.

Note: All Committee advisories and news releases are available on the World Wide Web at 'HTTP://WWW.HOUSE.GOV/WAYS__MEANS/'.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

NOTICE—CHANGE IN TIME

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON HEALTH

FOR IMMEDIATE RELEASE CONTACT: (202) 225–3943
July 16, 1999
No. HL–8–Revised

Change in Time for Subcommittee Hearing on Confidentiality of Health Information

Tuesday, July 20, 1999

Congressman Bill Thomas (R–CA), Chairman, Subcommittee on Health of the Committee on Ways and Means, today announced that the Subcommittee hearing on confidentiality of health information, previously scheduled for Tuesday, July 20, 1999, at 2:00 p.m., in the main Committee hearing room, 1100 Longworth House Office Building, **will now begin at 3:00 p.m.**

All other details for the hearing remain the same. (See Subcommittee press release No. HL–8, dated July 13, 1999.)

Chairman THOMAS. The Subcommittee will come to order. Well, good afternoon.

Today, the Subcommittee will be holding its second hearing on the confidentiality of health care information. The Ways and Means Committee began focusing on this issue directly and intently in 1996. That was the year Congress passed the Health Insurance Portability and Accountability Act or, as we call it, HIPAA.

Among HIPAA's many provisions was an initiative specifically designed to reduce the administrative costs associated with the processing of claims, other routine transactions, Medicaid, Medicare and the rest of the health care system. This initiative now codified in title XI of the Social Security Act is known as administrative simplification.

Part of that administrative simplification effort, in addition to standardized health care transactions, was acknowledgment that there was a need for re-evaluation and enhancement of the confidentiality protections afforded health information, particularly in light of stories and knowledge dealing with computers and the electronic forms of communication that began advancing themselves in the health care financing system.

We did that by including a provision in that administrative simplification section requiring the Secretary of Health and Human Services to develop and forward to the Ways and Means Committee

and the Senate Finance Committee recommendations for national health care confidentiality legislation. Those recommendations were forwarded to us in September 1997, and they were a subject of this Subcommittee's hearing last spring.

Now, there is an aspect of HIPAA that says unless Congress acts on the confidentiality legislation on its own by August 21 that the Secretary has the authority to promulgate regulations to protect confidentiality of information transmitted electronically. I think all of us hope that this will not be necessary. As the administration has often said, and I believe is sincere, it would be far better if Congress acted on the HIPAA mandate and passed a comprehensive confidentiality statute than regulations promulgated by the Secretary in accordance with the HIPAA provisions.

We have all been working on this issue. The Senate has labored, other Committees of the House have labored, and many of you know I have been working with a number of our colleagues, principally Ben Cardin, in the hopes of developing a bill that can be widely supported by Members on both sides of the aisle, by those who are involved in this issue and, most importantly, by providers and patients.

We believe we are close to presenting the Subcommittee with the proposal, but we believe this hearing will be very informative and will assist us in understanding some of the areas that we still have not been able to finalize. And more specifically today, we will be looking at the many different ways that personal health information is used in Medicare and throughout the private health care system. We will be looking at the Secretary's proposed policy under HIPAA, and I do think, though, many of the hearings that we have had for background and resource information are valuable, this one could be one of the most valuable ones that we will hold.

Our failure to act in this area may, in fact, miss a window to protect the confidentiality of patients' personal health information in a broad and significant way for individuals but just as importantly for health care outcomes research using the material that a confidentiality Federal structure would provide.

And so, I look forward to the testimony from our witnesses and look forward to Members of this Subcommittee meeting and trying to resolve what I think is one of the key issues today and that is identify and develop policies that balance truly competing needs, almost competing rights. This hearing will be central in assisting us in doing that, and I will recognize my colleague if he has any statement.

Mr. KLECZKA. Thank you, Mr. Chairman.

Mr. Chairman, what I would like to do is ask unanimous consent to enter into the record the opening statement by the Ranking Member, Pete Stark, who is under the weather today.

Chairman THOMAS. Without objection.

[The opening statements follow:]

Opening Statement of Chairman William M. Thomas, a Representative in Congress from the State of California

Good Afternoon. Today the Subcommittee will be holding its second hearing on the confidentiality of health care information. The Ways and Means Committee began its focus on this issue most recently, in 1996. That was the year Congress passed the Health Insurance Portability and Accountability Act, or HIPAA. Among HIPAA's many provisions, was an initiative specifically designed to reduce the ad-

ministrative costs associated with the processing of claims and other routine transactions in Medicare, Medicaid and the rest of the health care system. This initiative, now codified in Title XI of the Social Security Act, is known as Administrative Simplification.

As part of the Administrative Simplification effort, Congress acknowledged that, in addition to standardized health care transactions, there was a need for a reevaluation and enhancement of the confidentiality protections afforded health information—particularly in light of the increasing use of computers and electronic forms of communication in the health care financing system. Congress did this by including in the Administrative Simplification provisions a requirement that the Secretary of Health and Human Services develop and forward to the House Ways and Means and Commerce Committees, and the Senate Finance and Labor Committees, recommendations for national health care confidentiality legislation. The Secretary's recommendations were forwarded to us in September of 1997 and they were the subject of our last hearing on this issue last Spring. Unless Congress acts on confidentiality legislation of its own by August 21st of this year, the HIPAA law gives the Secretary the authority to promulgate regulations to protect the confidentiality of information transmitted electronically in connection with one of HIPAA standardized transactions.

I hope that this will not be necessary. As the Administration has often said, I believe it would be far better if Congress acted on the HIPAA mandate and passed a much, more comprehensive confidentiality bill—a bill that would protect the confidentiality of all personal health information in the system—not just that transmitted in accordance with HIPAA.

That is why I am intent on bringing legislation before this panel shortly that will meet the HIPAA mandate and go beyond, and establish protections for all personal health information. As many of you know, I have been working with my colleague, Representative Cardin, in the hopes of developing a bill that can be widely supported by Members on both sides of the aisle. While I believe we are close to presenting the subcommittee with a proposal, I believe this hearing will be very informative and help us greatly as we seek to hammer out the final details.

More specifically, today we will be looking at the many different ways that personal health information is used in Medicare and throughout our private health care system. Moreover, we will be examining the possible effects of the Secretary's proposed policy to protect the confidentiality of that information. As far as I am concerned, the importance of this issue to health policy can not be overstated. Confidentiality is a fundamental value of medicine. It is essential to the delivery of care. Only by honoring the confidences of patients can the system maintain the trust that is critical to the patient-caregiver relationship. Only by protecting the confidentiality of patient's personal health information can we ensure that patients will continue to seek out care when needed.

Similarly though, information about individual patient encounters with the health system is of fundamental importance to efforts to our improve the public health. The lessons learned from one patient's encounter with the system makes it possible to improve the care of the next patient. Finding new cures for disease and identifying better methods of treatment are dependent on information that is learned when patients obtain care. Finally, information about individual patient encounters is essential to the processing of today's increasingly complex and sophisticated payment arrangements—including those we employ today to finance Medicare and Medicaid.

Our challenge is to identify and develop policies that balance these competing needs. My hope is that today's hearing will be instrumental in helping us do this.

Opening Statement of Hon. Fortney Pete Stark, a Representative in Congress from the State of California

Thank you, Mr. Chairman, for holding this hearing today.

We have a lot of questions to ask our witnesses. They are difficult questions that many committees have struggled to answer over the course of numerous hearings during the last several years.

I hope we can make progress today by getting some thoughtful answers to some of the toughest issues in the medical privacy arena. The most fundamental is this: Does federal legislation that establishes uniform rules for all health care providers have to preempt state laws?

I submit that the answer is no—that under the federal Supremacy Clause that we will shortly be hearing more about from GAO, any confidentiality legislation we enact will become a baseline for medical privacy in this country. This means that

if federal law is more protective than similar state laws, then our legislation will become the standard. And the degree of public anxiety about eroding medical privacy tells me that any federal standard should be as clear and as protective as possible.

But in those cases where a state's law is stronger—as in California's requirement that all law enforcement officials must have a warrant to access identifiable health information—then state law should govern.

If followed, this basic principle would provide meaning and shape to a debate that has often sputtered and bogged down over definitional squabbles that fail to produce a workable agreement.

We have little enough time left to craft a consensus. And I regret that the panel's real expert on medical privacy, Dr. Jim McDermott, is not able to be with us today. As yet, we do not have legislation under consideration by this Subcommittee. But I hope that when we do, we will have plenty of time to discuss it and ask further questions before marking it up.

Thank you.

Mr. KLECZKA. And also the statement of another colleague from the Subcommittee, Jim McDermott, who has been very active in this issue. He is unable to be here. He is recuperating from heart surgery back in his home State of Washington.

I talked to Jim a short time ago, and he is doing quite well, and he thanks all the Members of Congress for their concern and the friends that he has around the DC area.

So I would ask unanimous consent that Mr. McDermott's statement be entered also in the record.

Chairman THOMAS. Without objection.

[The opening statement follows:]

Statement of Hon. Jim McDermott, a Representative in Congress from the State of Washington

Mr. Chairman, thank you for inserting my statement into the record. I had hoped to be here for this hearing, but I am in Seattle recuperating from heart surgery.

As you know, medical privacy is an issue that I have long cared about. As a psychiatrist and health care consumer I witnessed a need for strong federal privacy law protecting patients. It is amazing that we don't have strong privacy protections in place for medical records already yet we have one for video rental records.

Why do we need a Federal medical privacy law? Currently, privacy protections are weak and vary widely from state to state. Only 28 states allow people to even examine their own medical records. This lack of strong national standards could allow employers, schools, marketing agencies and others access to what ought to be confidential files.

Ensuring privacy in medical care is more important now than ever before because of new technologies like genetic testing and the computerization of medical records. Genetic research and testing has profound implications for our country's health care system because genetic information discloses not just our current health, but also purports to accurately predict our potential future health, and the health of our families.

The Human Genome Project may have a draft of the entire genome by early next year. And, in the near future, tests will be available for common genetically affected conditions. These tests create opportunities even as they raise serious challenges that we need to address immediately.

The BRCA–1 genetic test for breast cancer illustrates the dimensions of this debate. Women have been advised to be tested, but only as part of a research protocol.

Some patients see this as paternalistic, preferring to be informed of the results of the test, even if those results are not easily interpretable at this moment. Patients are warned about the potential risks of whether they will be able to buy health insurance or even if they will be able to get a job—should others learn of

their genetic status. Understandably, this has discouraged some women from participating in even the research, where their identities should be strictly protected.

Not everyone wants to know his or her genetic status. This can cause friction for families in which some members wish to be tested, but others do not. Sometimes the tests require participation by several family members to determine which mutation is common in that particular family. Some mothers have opted not to be tested to prevent anticipated discrimination against their daughters, while others feel compelled to be tested to spare their daughters the anxiety of not knowing if they carry the mutation.

Genetic tests also raise the issue of cost. Many insurance plans do not cover genetic tests, or they do not cover the counseling that is an integral part of genetic therapy. If a woman has no health insurance, frequent mammography screenings for breast cancer are a considerable expense, and the results of the test may be worse than useless to her.

Increasing reliance on mass computer databases further complicates the problem. Computers have revolutionized the way an individual's medical information is collected, stored, and disseminated. Without adequate, enforceable controls, this information can be used to breach the privacy of patients and to discriminate against them.

In 1995, Harvard and Stanford conducted a study of 200 people who suffered discrimination in insurance, jobs, education, or child adoptions because of their predisposition to a genetic disease. What makes their stories particularly disturbing is that these people had no symptoms, and perhaps would never develop that particular disease. These examples led to my concern about what the future holds if we allow indiscriminate use of these new technologies.

I will introduce this year, as I have in the last two congresses, a bill called the "Medical Privacy in the Age of New Technologies Act." This measure is intended to ensure that a patients personal health information will not be disclosed without that patients explicit consent, and that patients have access to their own records. It puts the individual in charge of what happens to his or her medical information, who sees it, and why.

As you may know, the Congress is required to pass privacy legislation by this August. If we fail to meet this deadline, the Secretary of Health and Human Services will promulgate regulations. Even the Secretary agrees that regulations will not provide patients with the kind of strong protections that can be imposed by law.

As the Subcommittee considers legislative proposals there are two basic principles that should be included in any privacy legislation:

• First, people need to be notified of how their personal information might be used,

• Second, they must have the opportunity for meaningful informed consent. Informed consent in the realm of health care is key. If patients fear that their records will be used in ways they do not know about, or will be given to third parties without their permission, they will not trust the health care system, and they will not tell their doctors the information necessary to provide them the best care.

It is likely that the generalizations we use to describe competing privacy proposals will make the bills sound very similar. But, to use an often-overused phrase, the devil is in the details. When you examine the details of these bills you will find a number of distinctions. Most notably they differ on the issues of the informed consent, research, and the preemption of state laws.

Following the basic principle that an individual has a right to privacy of their health information, it is important the patient is informed—in writing—of what information is to be disclosed, for what purpose, to which entity, and for what period of time. There should be two tiers of authorization: one for treatment and payment, and another for other purposes, such as research. Individuals can not "opt out" of using their information for treatment and payment. However, in some bills including my own, patients can opt out of using their information for the second tier "other purposes." The debate in Congress has focused around what constitutes "treatment and payment." Does treatment and payment include auditing, research, marketing, and so on?

Research is another area of distinction. How will medical privacy legislation affect the ability to conduct medical research? The legislation I have proposed will not undermine research capabilities. It allows researchers to use coded information, meaning information that either is anonymous, but could be linked to protected health information by authorized persons, or is nonidentifiable information, which is anonymous and cannot be linked to anyone. Some legislation, such as the Bennett bill, has taken the approach that since we have all benefited from past medical research we are obligated to participate in future research. This is a tremendously important

and difficult area to legislate. For which reason, I am working to find a balance between the two approaches.

One of the most contentious issues we are grappling with is the issue of pre-emption of state law. I believe that the only meaningful medical privacy law will be one that is a "federal floor" that does not pre-empt stronger state laws. There are literally thousands of state laws that address the privacy of medical records information in non-health related areas. The pre-emption of all state law could have significant unintended consequences and will be costly to states. For instance, laws are on the books in many states regarding the privacy of the health information of victims of sexual assault. To broadly pre-empt these laws—not knowing what we are pre-empting and what the impact will be—is very short sighted.

To argue the necessity of a "federal ceiling" claiming that we must preempt state laws to make it easier for the interstate health industry is incredible. For a Congress that has advocated sending power back to the states, I find it ironic that in this case they think the Federal government can do it better. Restricting states from passing stronger privacy laws would keep them from responding to many new, unique, and inherently local challenges in health care and public health. Especially, since there is no precedent in federal privacy or civil rights law for pre-empting stronger state laws.

In the coming debate, many people will speak for industries that stand to make money from the use and misuse of information. For them, medical records are commodities that are bought and sold.

We will hear many claims that any new legislation must not interfere with those particular interests. But the group we should listen to most will be hardest to hear: patients and their families. Think about your own family's medical records being available for anyone to look at. What value can we place on the confidentiality of the doctor-patient relationship? It is essential that we protect the privacy of individuals, including their genetic privacy. Good legislation can ensure that new technologies are used, not to deny health care or to deny medical privacy, but to benefit all of us.

Thank you.

Opening Statement of Hon. Jim Ramstad, a Representative in Congress from the State of Minnesota

Mr. Chairman, thank you for calling this important hearing to discuss the confidentiality of medical records.

Given the sensitive nature of personal health records, I am very aware of the importance of crafting appropriate legislation, as well as the complexities that surround this task. As Americans, we greatly value our personal privacy. As the world leaders in innovative and quality health care, we also understand the need to use some information in ways that promote research and development and quality assessments, as well as prevent fraud and abuse.

Since this Subcommittee is charged with the responsibility of overseeing the Medicare program, I especially appreciate this hearing's attention to the privacy of personally identifiable information for the 39 million Americans enrolled in that important health care program.

The General Accounting Office (GAO) will testify today about the importance of using personally identifiable information for the proper operation of the Medicare program, as well as the effect of state restrictions on HCFA's behavior. My constituents and I certainly look forward to learning more about HCFA's policies and practices regarding the disclosure of information, as well as HCFA's plans to improve the adequacy of its confidentiality safeguards and monitoring activities.

Again, thank you for calling this important hearing. I look forward to learning more from our witnesses about the confidentiality of all medical records.

Mr. KLECZKA. Mr. Chairman, I just want to say a couple of things on the issue of privacy.

It is an area where I have had concerns for years now. This is the second session that I have introduced my Personal Information Privacy Act which indicates that a person's privacy is theirs and should not be waived or given away.

I know the Chairman would like to have something done by the Committee on medical privacy, hopefully by the Congress before the August. However, I would caution the Committee against rushing and passing a bill that does not truly protect the privacy of the individual. Some of the things I have read and heard about which concern me are legislation preempting States' laws in this area, and provisions where a person who doesn't give a blanket waiver for release of their health care records could be denied health care services. You know, I am hopeful that those rumored provisions won't be in the final bill, but they disturb me greatly. I don't think there are competing interests with my health care privacy. It is mine. It is my medical record. It is my background. It is my past. I paid, along with the insurance company, for the medical care described in my records. We have gotten to the point in this country where we don't recognize these important facts.

I happened to go to a new dentist in my home district of Milwaukee, Wisconsin, and I was filling out the elongated form before he looked at my mouth, and on the form he asked for my Social Security number. Well, what does my Social Security number have to do with my teeth? I think it has a lot more to do with my tax liability and the interest I get from my bank, so I left that blank.

Then there was another section of the application where he asked whether or not he or the office could release this information. It didn't indicate for what purpose, but he wanted my blanket authorization to release the status of my teeth or my root canals to anyone he deemed appropriate to receive that information. There again I left that blank, and I think the consumer should have those rights.

And the upshot, Mr. Chairman, was he treated me. Well, he didn't really treat me. He gave me an evaluation. The treatment comes this Friday, and $1,300 later I am going to be "more better". But, nevertheless, whatever is in that office and in my file is between my dentist and myself and my mouth. I don't think it should be shared on the Internet; it should not be shared with the world.

If, in fact, somebody wants to do a clinical evaluation of Kleczka's teeth, they should ask me; and at that point I would probably say yes because, you know, I have no special teeth. But I think the legislation that we develop in this Subcommittee or in this Congress should recognize that the ultimate right of privacy is with the patient, is with the consumer, and I would not be willing, through my vote, to give away that right to any researcher, to any insurance company or to anyone else.

Thank you, Mr. Chairman.

Chairman THOMAS. I thank the gentleman.

If the first panel would come forward. The panel consists of Peggy Hamburg, M.D., Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services; Michael Hash, Deputy Administrator at HCFA; and Leslie Aronovitz, who is the Associate Director of Health Financing and Public Health Issues, Health, Education, and Human Services Division, United States General Accounting Office.

Your written testimony will be made a part of the record. In the time that you have available you may address us in any way you

see fit; and between the two of you, Mr. Hash, Honorable Hamburg, you can work out which one goes first.

Mr. HASH. I will be happy to go first.

Chairman THOMAS. So we will start with you and move across the panel. Thank you very much.

STATEMENT OF MIKE HASH, DEPUTY DIRECTOR, HEALTH CARE FINANCING ADMINISTRATION, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. HASH. Thank you, Chairman Thomas and Members of the Health Subcommittee. We appreciate the opportunity to come and testify about our efforts to improve protections for personally identified beneficiary information that is in our program's possession.

No administration has been more committed to protecting medical privacy. President Clinton and Vice President Gore have both spoken about its paramount importance. We provide much greater protection for sensitive personal health information in our programs than does the private sector. We strive to continually enhance our protections, and we greatly appreciate the evaluations and the advice of our Office of Inspector General at HHS, as well as the General Accounting Office.

As the GAO has confirmed in its report to you, personally identifiable information on Medicare beneficiaries is essential to the operation of the program. We need it to make accurate payments in the fee-for-service portion of Medicare and to risk adjust the Medicare+Choice payments so that they take into account individual beneficiary health status information and reduce any disincentives for the enrollment of sicker beneficiaries.

We also need personally identifiable information to conduct medical reviews and other activities that are essential to fighting waste, fraud and abuse in our programs.

We certainly need it to coordinate benefits and ensure that we do not pay for claims that other insurers are liable to pay.

And of course, we need it to protect—or to project, I should say, spending trends to accurately determine premium amounts for the Medicare Program, to develop and refine policies, including payment policies; to assess and improve quality and access; and last but far from least, we need to be responsive to individual beneficiary inquiries about coverage and payment affecting their interests.

Medicare data are also an invaluable asset in the efforts to improve care and coverage for beneficiaries by our research colleagues at the National Institutes of Health, the Agency for Health Care Policy and Research, and other scientific investigators and policy analysts.

Equally essential is our obligation to protect sensitive beneficiary information and to clearly inform beneficiaries of how information about them will be used in accordance with the requirements of the Privacy Act. Whenever concerns are raised about privacy, we take them seriously and we act on them immediately.

That is what we did earlier this year when Vice President Gore and a number of Members of Congress identified potential problems with our home health patient Outcome and Assessment Information Set known as OASIS. As you may recall, we halted imple-

mentation of the use of that instrument and conducted a thorough review of it. We made some important modifications to ensure that only essential information would be collected and that it would be properly protected, and we made sure that beneficiaries would be fully informed on why it is being collected and how it would be used.

Because protecting beneficiary information is essential to our mission, we are taking several new steps to strengthen our efforts.

First, we have established a new Beneficiary Confidentiality Board to provide executive leadership in all aspects of privacy protection.

Second, we are reviewing all of our beneficiary notices to ensure that they fully disclose in plain language how data collected from individual beneficiaries is to be used.

Third, we are designing new systems that will easily track when and where the data are shared.

Fourth, we are increasing efforts to ensure that researchers and Medicare contractors have properly protected patient data.

And, finally, we have introduced a system security initiative across HCFA to aggressively address vulnerabilities that have been found through the Inspector General's investigations and our own reviews.

The new steps we are taking can only strengthen our solid track record of protecting confidential beneficiary information. Our new Beneficiary Confidentiality Board in particular will provide an overarching executive level focus on our obligation to remain vigilant in this area. We encourage continuing oversight by the Inspector General's Office and by our colleagues at the General Accounting Office and others to help us address any new privacy concerns promptly, and we remain committed to swiftly addressing any related issue or breaches that might occur.

Mr. Chairman, thank you for this opportunity to discuss these issues; and I look forward to answering any questions that you or other Members of the Subcommittee may have.

[The prepared statement follows:]

Statement of Mike Hash, Deputy Director, Health Care Financing Administration, U.S. Department of Health and Human Services

Chairman Thomas, Congressman Stark, distinguished Subcommittee members, thank you for inviting us to testify about our efforts to improve protections for personally identifiable beneficiary information. No Administration has been more committed to protecting medical privacy. President Clinton and Vice President Gore have both spoken about the paramount importance of medical records privacy.

We provide much greater protection for sensitive information than does the private sector. We strive to continually enhance our protections. And we greatly appreciate the evaluations and advice of the HHS Inspector General (IG) and the General Accounting Office (GAO) in this regard.

As the GAO recently confirmed, personally identifiable information on Medicare beneficiaries is essential to the operation of the Medicare program. We need it to:

- make accurate payments in fee-for-service and to risk adjust Medicare+Choice payments so they take into account individual beneficiaries health status and curtail the disincentive for plans to enroll sicker beneficiaries;
- conduct medical reviews and conduct other activities essential to fighting fraud, waste and abuse;
- coordinate benefits and ensure that we do not pay claims for which other insurers are responsible;
- project spending trends and accurately determine premium amounts;
- develop and refine policy to ensure proper coverage and payment;

• assess and improve quality and access to care, for example by monitoring and then working to increase the number of beneficiaries receiving an influenza vaccination; and,

• be responsive to individual beneficiary inquiries about coverage and payment.

Medicare data are also an invaluable asset in efforts to improve care and coverage for beneficiaries by our research colleagues at the National Institutes for Health, the Agency for Health Care Policy and Research, and other scientific investigators and policy analysts.

It is equally essential that we protect the sensitive beneficiary information with which we are entrusted, and that we clearly inform beneficiaries of how information about them is used in accordance with the Privacy Act. Whenever concerns are raised about privacy, we take immediate action to address them.

For example, when Vice President Gore and members of Congress identified potential problems with our home health patient Outcome and Assessment Information Set (OASIS) earlier this year, we halted implementation, conducted a thorough review, and made important modifications to ensure that only essential information would be collected, that it would be properly protected, that disclosures would be limited to the minimum necessary to carry out HCFA's mission, and that beneficiaries would be fully informed on why it is being collected and how it will be used.

Because protecting beneficiary information is essential to our mission, we are taking several new steps to strengthen our efforts.

• We have established a new Beneficiary Confidentiality Board to provide executive leadership in all aspects of privacy protection.

• We are reviewing all beneficiary notices to ensure that they fully disclose in plain language how data are used.

• We are designing new systems that will easily track when and where data are shared.

• We are increasing efforts to ensure that researchers and Medicare contractors have properly protected data.

• And we have introduced a systems security initiative to aggressively address vulnerabilities found through the Inspector General's and our own reviews.

CONFIDENTIALITY BOARD

We have established a new Beneficiary Confidentiality Board to coordinate and consolidate privacy policies and ensure that we do not collect or disseminate more information than is absolutely necessary. The Board is led by the Director of the Center for Beneficiary Services and includes senior executives from all Agency components that have a direct stake in privacy and confidentiality, including the Center for Medicaid and State Organizations, the Center for Health Plans and Providers, the Office of Clinical Standards and Quality, the Office of Strategic Planning, the Program Integrity Group, the Office of Information Services, the Office of the Actuary, and Regional Office representatives. Core responsibilities include:

• establishing strategic goals, overarching policies, and objectives for protecting data;

• establishing, coordinating, and issuing all policy decisions on privacy and confidentiality;

• assuring implementation and enforcement of guiding principles for Agency-wide strategic goals and objectives;

• providing executive oversight of compliance with all privacy and confidentiality statutory and regulatory requirements, and assuring that beneficiary protections are enforced;

• reviewing all current operations with regard to systems of records and beneficiary protections to assure that strategic goals and objectives and guiding principles are in place and effective at all levels, including contractors to sub-contractors;

• evaluating legislative proposals involving the collection, use, and disclosure of personal information by any entity, public or private, for consistency with legal standards and our guiding principles;

• assuring that use of new information technologies sustains protections of information that directly identifies an individual or from which an individual's identity can be deduced;

• assuring that personal information contained in our systems of records are handled in full compliance with fair information practices as set out in the Privacy Act; and,

• serving as a senior-level forum for the discussion and resolution of key strategic issues affecting HCFA's privacy and confidentiality policies and implementation strategies.

This will help ensure a central focal point for privacy issues and accountability across all aspects of Agency business.

BENEFICIARY NOTICES

Beneficiaries need to know and understand why personally identifiable information is collected and how it is used. This is both a legal requirement and an ethical obligation. There are many different notices to beneficiaries about why information is collected and how it is used.

Some, including the newest notice for OASIS, has been carefully crafted to ensure that it is clear and comprehensive. However, we agree with the GAO that some of the earlier beneficiary notices do not meet the Privacy Act requirements to inform beneficiaries about:

- the authority under which we are collecting information;
- the principal purpose for which it will be used;
- the routine uses for which it may be used; and
- whether the individual is required to supply the information and what the consequences are if the individual does not supply the information

Earlier this year, we began a systematic review of all beneficiary privacy notices, rewriting them as necessary, to ensure that they provide full disclosure in plain language.

TRACKING DATA RELEASES

The Privacy Act stipulates that beneficiaries are entitled to know, upon request, any and all instances in which identifiable information about them has been shared. We have never had such a request, but have realized that complying with one would be extraordinarily labor intensive with our current information systems. It also is currently difficult to provide data on our Privacy Act compliance to the Office of Management and Budget (OMB) for its oversight responsibilities.

We are now working to fully define the requirements for information systems that will ensure full compliance with OMB and Privacy Act requirements. Implementing these systems is a top information technology priority once we have cleared the Year 2000 hurdle. In the interim, we have increased our surveillance of these requests and are improving our existing tracking systems to align them more fully with OMB requirements.

DATA USE OVERSIGHT

The data files we maintain are an invaluable asset to medical and health policy researchers in their efforts to improve beneficiary care and coverage. For example:

- we are able to share the extensive information we have on beneficiaries with end-stage renal disease directly with National Institute of Health scientists that they can use to study and improve treatment;
- the Agency for Health Care Policy and Research Patient Outcome Research Teams rely upon this beneficiary information to develop new insights on the treatment of the most frequent medical conditions affecting the elderly; and,
- the data files are also critical to investigators under contract to us for evaluation and development of payment, coverage and treatment policies.

The Privacy Act does allow for sharing data with researchers as long as their work promotes the Agency's mission, is compatible with the purpose for which the information was collected, and proper privacy protections are in place.

Many research needs are met by "public use files" that we readily make available, and from which any data that could identify individual beneficiaries is removed, including information that could be used to deduce an individual beneficiary's identity. Additional research needs are met by encrypted data files in which data elements that explicitly identify individuals (such as names, claim numbers, physician numbers, service dates, and date of birth) are either removed, encrypted, or stated as a range (of dates, for example). Some data elements remain in these files that could possibly be linked with other information to a deduce specific individual's identity. Finally, there are some valid research endeavors for which individually identifiable information is essential.

For all research requests, we conduct a careful review to ensure that any disclosure of information is allowed under the Privacy Act. For research projects outside of HHS, or not funded by HHS, we conduct another careful level of review to ensure that the request is for the bare minimum of information that is essential to a given research project, and that the project has scientific merit and sound research methodology. We are also diligent in making clear to researchers how data that could be used to identify individual beneficiaries must be protected.

When proper criteria are met, we develop data use agreements that contain explicit protections covering the release and use of data. These agreements also specify that the user must contact us within 30 days of completion of the approved project for instructions on whether to return all data files to us or to destroy such data and execute an attestation to certify the destruction. We have taken swift action to address the rare situations that we are aware of in which researchers have not fully complied with Privacy Act requirements and our data use agreements to clarify their responsibilities to protect beneficiary confidentiality.

We are now increasing efforts to verify that researchers have in fact complied with their data use agreements to protect data and dispose of it properly once projects are completed. We expect to reduce our backlog in half by the end of this fiscal year. We also look forward to working with the GAO and other experts to develop more systematic ways to proactively assure compliance with data use agreements so we can prevent problems before potential security breaches occur.

SYSTEMS SECURITY

We are also working to improve security in electronic data processing. We have introduced a systems security initiative to aggressively address vulnerabilities found through the Inspector General's and our own reviews. Our goal is to be able to maintain the tightest possible security as the business environment in which we operate changes, and to integrate security into every aspect of our information technology management activities.

One of the first things our new Chief Information Officer, Gary Christoph, did when he came on board was to hire outside experts to search out security weaknesses in our systems so we could proactively address them. We also have acquired new technology, beefed up staff training, conducted our own risk assessments and internal audits, and enhanced procedures for guarding access to sensitive systems. However, there are no silver bullets, and vigilance here must be constant given the ever changing nature of technology and evolution of new risks.

As we clear the Year 2000 hurdle and its demand on our systems, we will be able to increase our security even more through our comprehensive security initiative. We are now in the process of developing the protocols to systematically monitor the systems security of our claims processing contractors. The new evaluation process will specifically assess administrative, technical, and physical protection measures to protect beneficiary privacy.

We also have recently restructured our contractor oversight operations and initiated a new contractor evaluation process which will incorporate the security review findings and improve our overall management of the contractors. In addition, the Administration has proposed comprehensive contracting reform legislation that will bring Medicare contracting authority in line with standard Federal government contracting procedures and make it easier for us to terminate contractors if we find they are not providing adequate privacy protections.

We will continue to use the annual Inspector General CFO audits as an opportunity to identify threats to the integrity of our data systems and to ensure that we address vulnerabilities in a timely manner. We also are carrying out activities required by the Presidential Decision Directive 63, as well as security requirements in the Health Insurance Portability and Accountability Act, which will further strengthen our security protections.

CONCLUSION

The new steps we are taking can only strengthen our solid track record of protecting confidential beneficiary information. Our new Beneficiary Confidentiality Board, in particular, will provide an overarching executive-level focus on our obligation to remain ever vigilant. We encourage the IG, GAO, and others to also be vigilant in raising and helping us to address any concerns about protections for sensitive information. And we remain committed to swiftly and effectively addressing any related issues or breaches that might arise. I thank you again for holding this hearing, and I am happy to answer any questions you might have.

Chairman THOMAS. Thank you very much.

Doctor.

Dr. HAMBURG. Mr. Chairman.

Chairman THOMAS. Let me caution you that these microphones are very unidirectional, so you need to speak directly into it. Thank you.

STATEMENT OF HON. MARGARET A. HAMBURG, M.D., ASSISTANT SECRETARY FOR PLANNING AND EVALUATION, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Dr. HAMBURG. Thank you for this opportunity to appear before you to discuss the Secretary's recommendations for privacy legislation.

I would also like to emphasize the administration's support for passage of bipartisan legislation providing comprehensive privacy protection for people's health care information. Stories abound that raise concern that our sensitive medical information can enter the wrong hands and be misused. For example, at one HMO, every clinical employee could tap into patients' computer records and see notes from psychotherapy sessions. The director of a work site health clinic testified before the National Committee on Vital and Health Statistics that he was frequently pressed to disclose his patients' health information to their supervisors.

These kinds of problems underlie the legitimate fear that Americans have about the security of their health care information. Almost 75 percent of our citizens say that they are at least somewhat concerned that computerized medical records will have a negative effect on their privacy. If we don't act now, public distrust could deepen and ultimately stop citizens from disclosing important information to their doctors or from seeking needed medical testing or treatment, especially for sensitive concerns like mental illness or genetic disorders.

The problem is not theoretical. Numerous analyses over several years by government, industry and professional groups have identified serious gaps in protections for health information and have recommended Federal legislation to close them.

In September 1997, Secretary Shalala presented her recommendations for protecting the "confidentiality of individually identifiable health information." In that report the Secretary concluded that Federal legislation establishing a basic, national floor of confidentiality is necessary to provide rights for patients and define responsibilities of recordkeepers. She recommended that Federal legislation focus on health care payers and providers and the information they create and receive in providing and paying for health care.

The Secretary recommended legislation to implement five key principles:

First, information about a consumer that is obtained for delivering and paying for health care should, with very few exceptions, be used and disclosed for health purposes and health purposes only.

Second, those who legally receive health information should be required to take reasonable steps to safeguard it. They should ensure that the information is available only to those who should have access to it and only for purposes authorized by the patient or authorized by law.

Third, consumers should have access to their health records and should know how their health information is being used and who has looked at it. Consumers should be given a clear explanation of these rights.

Fourth, people who violate the confidentiality of our personal health information should be accountable. Those who use this information improperly should be punished.

These first four principles must, however, be balanced against the fifth principle, public responsibility. Just like our free speech rights, privacy rights cannot be absolute. We must balance our protection of privacy with our public responsibilities to support other critical national goals, public health, research, quality care and our fight against health care fraud and abuse.

Our Department is keenly aware of the need to use personal health information for each of these national priorities. For example, our researchers have used health records to help us fight childhood leukemia and to learn that beta blocker therapy results in fewer rehospitalizations and improved survival among elderly survivors of acute myocardial infarction or heart attack. Public health agencies use health records to warn of outbreaks of emerging infectious disease threats. And our efforts to improve quality in our health care system depend upon our ability to review health information.

As you know, HIPAA requires that if Congress fails to enact comprehensive privacy legislation by August of this year, HHS must implement final regulations by February of the year 2000. We have assembled a team from all of the relevant Federal agencies to work on these regulations, and it is our intent to have an NPRM, Notice of Proposed Rule Making ready for publication by fall. While we are moving ahead to have the regulation ready, the President and Secretary Shalala have made it clear that their first priority is to see Congress enact a comprehensive bill. Our staff have been working closely with many of your staff, and staff in the Senate, to assist in achieving this goal. We are eager to see legislation and want to work with you to make this happen.

Mr. Chairman, the principles embodied in our recommendations should guide a comprehensive law that will create substantive Federal standards and provide our citizens with real peace of mind. The principles represent a practical, comprehensive and balanced strategy to protect health care information that is collected, shared and used in an increasingly complex world.

Thank you again for giving me this opportunity to testify. I look forward to answering any questions that you may have.

[The prepared statement follows:]

Statement of the Hon. Margaret A. Hamburg, M.D., Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services

Mr. Chairman, Congressman Stark, distinguished members of the Committee: I appreciate the opportunity to appear before you to discuss the Administration's recommendations for federal legislation to protect the privacy of health information.

As you may remember, Secretary Shalala first presented her recommendations, required by the Congress under Section 264 of the Health Insurance Portability and

Accountability Act (HIPAA), in September 1997.[1] I think it is fair to say that the recommendations were well received and have been used to assist others in crafting their own legislative proposals.

HIPAA also requires that if Congress fails to enact comprehensive privacy legislation by August of this year, HHS must implement final regulations by February 2000. We have assembled an interagency team to work on the regulations including representatives from the Departments of Labor, Defense, Commerce, the Social Security Administration, the Veterans Administration and the Office of Management and Budget. It is our intent to have the regulations prepared in time to meet the statutory deadline.

While we are moving ahead to have the regulation ready, the President and Secretary Shalala have made it very clear that their first priority is to see Congress enact a comprehensive health information privacy bill. Our staff have been working closely with many of your staff, and staff in the Senate, to assist you in achieving that goal. Again, let me reiterate, we want to see legislation, and we want to work with you to make that happen.

The issue of health information privacy is quite complex—in order to resolve it legislatively, some difficult choices will have to be made. We believe that our recommendations strike the appropriate balance between the privacy needs of our citizens and the critical needs of our health care system and our nation. This is an issue that touches every single American, and to reach resolution we will need a bipartisan effort.

THE NEED FOR LEGISLATION

It has been 25 years since former HEW Secretary Elliot Richardson set forth principles that led to the landmark Federal Privacy Act. Those 25 years have brought vast changes in our health care system.

Revolutions in our health care delivery system mean that we must place our trust in entire networks of insurers and health care professionals—both public and private. The computer and telecommunications revolutions mean that information no longer exists in one place—it can travel in real time to many hospitals, physicians, insurers, and across state lines.

In addition, revolutions in biology mean that a whole new world of genetic tests have the potential to either help prevent disease or reveal the most personal health information of a family. Without safeguards to assure citizens that getting tested will not endanger their families' privacy or health insurance, we could endanger one of the most promising areas of research our nation has ever seen.

Health care privacy can be safeguarded. It must be done with national legislation, national education, and an on-going national conversation.

Currently, when we give a physician or health insurance company precious health information, the level of protection will vary widely from state to state. We have no comprehensive federal health information privacy standards. Because the practice of health care is increasingly becoming interstate through mergers, complex contractual relationships and enhanced telecommunications, we need strong federal standards. Establishing a baseline that provides uniformity will help reassure the public that they can trust their providers and insurers to keep their health information secure.

In developing our recommendations for federal legislation, we learned a great deal through consultations with a variety of outside groups and from six days of public hearings conducted by the National Committee on Vital and Health Statistics, our statutory federal advisory committee for health data and privacy policy. The hearings involved over 40 witnesses from across the health community, including health care professionals, plans, insurance companies, the privacy community, and the public health and research communities.

We believe our recommendations provide a balanced framework for legislation that can protect the privacy of medical records, guarantee consumers the right to inspect their records, and punish unauthorized disclosures of personal health data by hospitals, insurers, health plans, drug companies or others.

---

[1] "Confidentiality of Individually-Identifiable Health Information, Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996" can be found on the HHS web site at: <http://aspe.os.dhhs.gov/admnsimp/>.

THE PRINCIPLES

The Secretary's recommendations for legislation are grounded in five key principles: Boundaries, Security, Consumer Control, Accountability, and Public Responsibility.

Boundaries

The first is the principle of Boundaries: With very few exceptions, personally identifiable health care information should be disclosed for health purposes and health purposes only. It should be easy to use it for those purposes, and very difficult to use it for other purposes.

For example, employers should be able to use the information furnished by their employers to provide on-site care or to administer a health plan in the best interests of those employees. But those same employers should not be able to use information obtained for health care purposes to discriminate against individuals when making employment decisions—such as hiring, firing, placements and promotions. To enforce these boundaries, we recommend strong penalties for the inappropriate use or disclosure of medical records.

We recommend that the legislation apply specifically to providers and payers, and to anyone who receives health information from a provider or payer, either with the authorization of the patient or as authorized explicitly by legislation.

However, our recommendations acknowledge that these providers and payers do not act alone. In order for a provider or payer to operate efficiently, it may need to enlist a service organization to perform an administrative or operational function. For example, a hospital may hire an organization to encode and process bills, or a managed care organization may contract with a pharmaceutical benefit management company to provide information to pharmacists about what medications are covered and appropriate for their customers.

The numbers and types of service organizations are increasing every day. While most do not have direct relationships with the patients, they do have access to their personal health care information. Therefore, we recommend that they should be bound by the same standards. For example, a health plan's contractor should be allowed to have access to patient lists in order to do mailings to remind patients to schedule appointments for preventive care. But it should not be able to sell the patient lists to a pharmaceutical company for a direct mailing announcing a new product.

Because we recommend a minimum floor of protection for all records, our report does not distinguish among types of health care information based on sensitivity. For example, our recommendations do not include specific provisions related to genetic information in health records. Genetic information should be covered by the same rules. However, we recognize that the public is especially concerned about the unique properties of genetic information—its predictive nature, and its link to personal identity and kinship and its ability to reveal our family secrets.

Therefore while you are developing privacy legislation, you should also consider how to limit the collection and disclosure of genetic information and prohibit health insurers and employers from discriminating against individuals on the basis of their genetic information. Because of the speedy development of genetic technologies and its potential for abuse, we recommend that legislation concerning discrimination in underwriting by insurers or other improper use of such information be considered expeditiously. We look forward to continuing our work with you on this issue.

Security

The second principle is Security. Americans need to feel secure that when they give out personal health care information, they are leaving it in good hands. Information should not be used or given out unless either the patient authorizes it or there is a clear legal basis for doing so.

There are many different ways that private information like your blood tests could become public. People who are allowed to see it—such as lab technicians—can misuse it either carelessly or intentionally. And people who should not be seeing it—such as marketers—can find a way to access it, either because the organization holding the information doesn't have proper safeguards or the marketers can find an easy way around the safeguards. To give Americans the security they expect and deserve, Congress should develop legislation that requires those who legally receive health information to take reasonable steps to safeguard it and face consequences for failure to do so.

What do we mean by reasonable steps? The organizations should adopt protective administrative and management techniques, educate their employees, and impose disciplinary sanctions against employees who use information improperly.

We are addressing some of these steps in our Security Standards regulation, implementing the Administrative Simplification mandate under HIPAA. Our NPRM laid out a range of approaches for safeguarding the information to which the HIPAA mandate applies. However, that regulation will only cover the security of specific electronically maintained records. We need comprehensive privacy legislation to cover all health information that needs this kind of protection.

We don't believe a law can specify the details of these protections because each organization must keep pace with the new threats to our privacy and the technology that can either abate or exacerbate them. But a federal law can require everyone who holds health information to have these types of safeguards in place and specify the appropriate sanctions if the information is improperly disclosed.

Consumer Control

The third principle is Consumer Control. The principles of fair information practice (formulated in 1973 by a committee appointed by Secretary Richardson) included as a basic right: "There must be a way for an individual to find out what information about him is in a record and how it is used."

With very narrow exceptions, consumers should have the right to find out what is contained in their records, find out who has looked at them, and to inspect, copy and, if necessary, correct them. Consumers should be given a clear explanation of these rights and they should understand how organizations will use their information. Let me give you an example of why this is important. According to the Privacy Rights Clearinghouse, a California physician in private practice was having trouble getting health, disability, and life insurance. She ordered a copy of her report from the Medical Information Bureau—an information service used by many insurance companies. It included information showing that she had a heart condition and Alzheimer's disease. There was only one problem. None of it was true. Unfortunately, under the current system these types of errors occur all too often. Consumers often do not have access to their own health records and even those who do are not always able to correct some of the most egregious errors.

With that in mind, our recommendations set forth a set of practices and procedures that would require that insurers and health care providers provide consumers with a written explanation detailing who has access to their information and how that information will be used, how they can restrict or limit access to it, and what their rights are if their information is disclosed improperly.

We also recommend procedures for patients to inspect and copy their information, and set out the very limited circumstances under which patient inspection should be properly denied.

Finally, we recommend a process for patients to seek corrections or amendments to their health information to resolve situations in which innocent coding errors cause patients to be charged for procedures they never received, or to be on record as having conditions or medical histories that are inaccurate.

Accountability

The fourth principle is Accountability. If you are using information improperly, you should be punished. This flows directly from the second principle of security—the requirement to safeguard information must be followed by real and severe penalties for violations. Congress should send the message that protecting the confidentiality of health information is vitally important, and that people who violate that confidence will be held accountable.

We recommend that offenders should be subject to criminal felony penalties if they knowingly obtain or use health care information in violation of the standards outlined in our report. The penalties mandated in privacy legislation should be higher when violations are for monetary gain, similar to those Congress mandated in the administrative simplification provisions of HIPAA. In addition, when there is a demonstrated pattern or practice of unauthorized disclosure, those committing it should be subject to civil monetary penalties.

In addition to punishing the perpetrators, we must give redress to the victims. We believe that any individual whose privacy rights have been violated—whether those rights were violated negligently or knowingly—should be permitted to bring a legal action for actual damages and equitable relief. When the violation is done knowingly, attorney's fees and punitive damages should be available.

These first four principles—Boundaries, Security, Consumer Control and Accountability—must be carefully weighed against the fifth principle, Public Responsibility.

Public Responsibility

Just like our free speech rights, privacy rights can never be absolute. We have other critical—yet often competing—interests and goals. We must balance our pro-

tections of privacy with our public responsibility to support national priorities—public health and safety, research, quality care, and our fight against health care fraud and abuse and other unlawful activities.

Our Department is acutely aware of the need to use personal health information for each of these national priorities. For example, HHS auditors use health records to uncover kickbacks, overpayments and other fraudulent activity. Researchers have used health records to help us fight childhood leukemia and uncover the link between DES and reproductive cancers. Public health agencies use health records to warn us of outbreaks of emerging infectious diseases. In addition, our efforts to improve quality in our health care system depend on our ability to review health information to determine how well health institutions and health professionals are caring for patients.

For public health and safety, research, quality evaluations, fraud investigations, and legitimate law enforcement purposes, it's not always possible, or desirable, to ask for each patient's permission for access to the necessary health information. And, in many cases, doing so could create major obstacles in our efforts. While we must be able to use identifiable information when necessary for these purposes, we should use information that is not identifiable as much as possible.

To demonstrate how access must be balanced against public responsibility, let me outline a few of the areas in which we recommend that disclosure of health information should be permitted without patient authorization.

Public Health

Under certain circumstances, we recommend permitting health care professionals, payers, and those receiving information from them to disclose health information without patient authorization to public health authorities for disease reporting, adverse event reporting, public health investigation, or intervention. This is currently how the public health system operates under existing State and federal laws.

For example, consider the outbreak of E. coli in hamburger that resulted in the largest recall of meat products in history. Public health authorities, working with other officials, used personally identifiable information to identify quickly the source of the outbreak and thereby prevent thousands of other Americans from being exposed to a contaminated product.

Research

An important mission for the Department of Health and Human Services is to fund and conduct health research. We understand that research is vitally important to our health care and to progress in medical care. Legislation should not impede this activity.

Today the Federal Policy for Protection of Human Subjects and FDA's Human Subject Regulations protect participants in most research studies that are funded or regulated by the federal government. These rules have worked well to protect the privacy of individuals while not impeding the conduct of research. We recommend that similar privacy protections should be extended to all research in which individually identifiable health information is disclosed, and not just federally funded or regulated research.

All researchers must determine whether their research requires the retention of personal identifiers. There are research studies that can only be conducted if identifiers are retained; for example, outcomes studies for heart attack victims or the recent study which identified a correlation between the incidence of Sudden Infant Death Syndrome and the infant's sleep position. If, and when, personal identifiers are no longer needed, the researcher should be required to remove them and provide assurances that the information will be protected from improper use and unauthorized additional disclosures.

Under the Common Rule, if personal identifiers are necessary, an IRB must review the research proposal and determine whether informed consent is required or may be waived. In order for informed consent to be waived, an IRB must determine that the research involves no more than minimal risk to participants, that the absence of informed consent will not adversely affect the rights or welfare of participants, and that conducting the research would be impracticable if consent were required. This or a similar mechanism of review should be applicable for all research using individually identifiable health information without informed consent regardless of funding source.

This recommendation is consistent with the Federal Policy for the Protection of Human Subjects as well as the Privacy Act—policies that have protected federal research participants and research records for a quarter of a century and that have saved lives and fostered countless improvements in medical treatment.

PREEMPTION

Our recommendations call for national standards. But, we do not recommend outright or overall federal preemption of existing State laws that are more protective of health information.

Some protections that we recommend may be stronger than some existing State laws. Therefore, we recommend that Federal legislation replace State law only when the State law is less protective than the Federal law. Thus, the confidentiality protections provided would be cumulative and the Federal legislation would provide every American with a basic set of rights with respect to health information.

CONCLUSION

Mr. Chairman, the five principles embodied in our recommendations—Boundaries, Security, Consumer Control, Accountability, and Public Responsibility—should guide a comprehensive law that will create substantive federal standards and provide our citizens with real peace of mind.

The principles represent a practical, comprehensive and balanced strategy to protect health care information that is collected, shared, and used in an increasingly complex world.

In addition to creating new federal standards, we must ensure that every single person who comes in contact with health care information understands why it is important to keep the information safe, how it can be kept safe, and what will be the consequences for failing to keep it safe. Most of all, we must help consumers understand not just their privacy rights, but also their responsibilities to ask questions and demand answers—to become active participants in their health care.

We cannot expect to solve these problems all at once. With changes in medical practices and technology occurring every day, we need to be flexible, to change course if our strategy isn't working and meet new challenges as they arise.

Mr. Chairman, we in the Department and the Administration are eager to work with you to enact strong national medical privacy legislation.

Thank you again, for giving me this opportunity to testify. My colleagues and I look forward to answering any questions that you may have.

Chairman THOMAS. Thank you very much, Doctor.

Ms. Aronovitz.

STATEMENT OF LESLIE G. ARONOVITZ, ASSOCIATE DIRECTOR, HEALTH FINANCING AND PUBLIC HEALTH ISSUES, HEALTH, EDUCATION, AND HUMAN SERVICES DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Ms. ARONOVITZ. Mr. Chairman and Members of the Subcommittee, we are pleased to be here today as you discuss the various issues associated with protecting the privacy of personally identifiable information.

For the last several months, we have been studying the manner in which HCFA protects personally identifiable health information it collects on Medicare beneficiaries, and we are releasing our report today at this hearing.

Mr. Hash has mentioned some of the initiatives HCFA is undertaking. I would like to step back a bit and provide some information on our study.

To carry out its legislative responsibilities, HCFA needs to collect and maintain personally identifiable information on its 39 million Medicare beneficiaries. For example, it needs personally identifiable information about beneficiaries' demographics, enrollment and utilization of health care services to pay claims, determine the initial and ongoing eligibility of beneficiaries and review the care beneficiaries receive in terms of access, appropriateness and qual-

ity. HCFA also uses this information in essential research activities that can lead to improvements in rate setting, services provided, and quality of care.

We found that HCFA's policies and practices regarding disclosing personally identifiable health information are generally consistent with the provisions of the Privacy Act. When beneficiaries first sign up for Medicare and then when they receive care or participate in a demonstration project, for example, they receive notices that to different degrees include a discussion about how their information might be used. HCFA may disclose information without an individual's consent under certain circumstances such as for research purposes or authorized civil and criminal law enforcement activities.

In determining the validity of specific data requests, HCFA attempts to balance the needs of the requesters with the need to protect a beneficiary's confidentiality. Therefore, the agency would screen requests for sensitive information from non-HCFA researchers more thoroughly than it would from HCFA staff who need the data to conduct the agency's business.

We did identify, however, some areas where HCFA needs to do a better job to assure that personally identifiable information is not intentionally or inadvertently shared with those not authorized to have it. Specifically, the HHS OIG continues to find vulnerabilities in HCFA and its contractors' management of electronic information that could lead to individuals reading, disclosing or simply tampering with confidential information. In addition, because HCFA does not routinely monitor contractors and others who obtain such sensitive information, it cannot assure that those organizations are maintaining the information in a safe manner.

This being said, we found that HCFA has actually received very few complaints about Privacy Act violations to date. Nevertheless, HCFA officials told us that they are in the process of addressing the OIG's findings, to the extent that resources permit, given the need to focus on Y2K computer requirements in the short term, and that they are stepping up their oversight efforts at their Medicare contractors to assure that these organizations have established and are implementing a sound security plan.

In regard to providing beneficiaries an accounting of the disclosures it makes, which is a capability called for by the Privacy Act, we found that HCFA would be hard pressed to do so without a lot of effort. We also believe that HCFA could do a better job in informing beneficiaries of the purposes to which their information may be disclosed. To address these issues, as Mr. Hash has mentioned, HCFA has established a new executive Beneficiary Confidentiality Board and initiated a number of actions in response to January 1999, OMB guidance to all agencies to review information practices for compliance with the Privacy Act.

The last area we looked at was the potential effect on HCFA of State laws governing privacy. We found that some States prohibit the disclosure of sensitive health-related information except for very specific purposes. HCFA's practice has been to respect State laws to the extent possible when these laws are more restrictive than the Federal law. HCFA officials told us that these State laws have not prevented the agency from receiving information necessary for paying claims but may change its policy as the agency

develops and implements payment systems that depend on diagnostic information.

If HCFA had to comply with the myriad of State laws governing the receipt and use of health information, its ability to set rates, monitor quality and conduct and support health-related research could be hampered.

Currently, unlike the private sector, HCFA can invoke the Supremacy Clause of the U.S. Constitution to get information it needs to carry out its mission without regard to State requirements, although it has not done so to date.

Mr. Chairman, this concludes my prepared statement, and I also would be very happy to answer any questions you or the other Members of the Subcommittee might have.

[The prepared statement follows:]

Statement of Leslie G. Aronovitz, Associate Director, Health Financing and Public Health Issues, Health, Education, and Human Services Division, U.S. General Accounting Office

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss how the Health Care Financing Administration (HCFA) protects personally identifiable health information on Medicare beneficiaries. HCFA, an agency of the Department of Health and Human Services (HHS), possesses the nation's largest collection of health care data, with information on 39 million Medicare beneficiaries. To operate the Medicare program, HCFA must collect personally identifiable information on Medicare beneficiaries, such as their names, addresses, and health insurance claims numbers, as well their diagnostic and treatment information. HCFA uses this information for a variety of purposes, including paying approximately 900 million Medicare claims annually and conducting health-related research to improve quality of care. When a person signs up for Medicare, he or she might not realize the variety of uses HCFA makes of his or her personally identifiable information or that this personal information may legitimately be disclosed by HCFA outside the agency.

The personally identifiable information that HCFA collects on Medicare beneficiaries is protected by the Privacy Act of 1974. This law, which governs the collection, maintenance, and disclosure of federal agency records, balances the government's need to maintain information about individuals with their right to be protected against unwarranted invasions of their privacy. State laws also protect the privacy of certain personally identifiable medical information, and vary significantly in their scope and specific provisions. To create a more uniform set of protections, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that, unless Congress enacts a health privacy law establishing standards for the electronic exchange of health information by August 21, 1999, HHS must promulgate such standards within the following 6 months.

Today, we are releasing a report you requested that focuses on four areas related to HCFA's use of personally identifiable information.[1] They are:

- HCFA's need for personally identifiable health information to manage the Medicare program;
- HCFA's policies and practices regarding disclosure of information on Medicare beneficiaries to other organizations;
- The adequacy of HCFA's safeguards for protecting the confidentiality of electronic information and its monitoring of other organizations that obtain information on Medicare beneficiaries; and
- The effect on HCFA of state restrictions on the disclosure of confidential health information.

To develop our findings, we interviewed HCFA officials and reviewed documents HCFA provided on its confidentiality policies and procedures. We also reviewed guidance from the Office of Management and Budget (OMB) related to the Privacy Act, financial statement audits of HCFA from the HHS Office of Inspector General (OIG), and HCFA's plan for addressing problems identified in OIG audits. In addition, we examined the privacy protections of a number of state laws and obtained

[1] *MEDICARE: Improvements Needed to Enhance Protection of Confidential Health Information* (GAO/HEHS–99–140, July 20, 1999).

comments from HCFA officials about the effects of such laws on the management of the Medicare program.

In summary, we found that personally identifiable information on Medicare beneficiaries is vital to the operation of the Medicare program, and that HCFA can disclose such information to other organizations consistent with provisions of the Privacy Act. HCFA has policies and procedures for evaluating requests for disclosure of personally identifiable health information, but HCFA's confidentiality practices have a number of weaknesses. These weaknesses include HCFA's inability to easily provide beneficiaries with an accounting of disclosures made of their personal information and failure to always give them clear notification of the purposes for which their personal information may be disclosed outside of HCFA as required by the Privacy Act. Although few complaints of violations have been reported to date, the HHS OIG also continues to report vulnerabilities in HCFA's safeguards for confidentiality of electronic information. These vulnerabilities could lead to unauthorized individuals reading, disclosing, or altering confidential information. Finally, potential conflicts exist between HCFA and state laws regarding the disclosure of sensitive health information. To date, conflicts have been minimal and the administration of Medicare has not been hindered, according to HCFA officials, because all states permit release of information for health care treatment and payment. However, if the same data elements were not available from all states, it might compromise HCFA's ability to conduct research and analysis to improve Medicare policies.

BACKGROUND

In protecting the confidentiality of beneficiaries' health information, HCFA's activities, like those of other federal agencies, are governed by the Privacy Act of 1974. The Privacy Act requires that agencies limit their maintenance of individually identifiable records to those that are relevant and necessary to accomplish an agency's mission. Federal agencies store personally identifiable information in systems of records. A system of records is a group of records under the control of a federal agency from which information can be retrieved using the name of an individual or an identifier such as a number assigned to the individual. The Privacy Act defines a record as any item, collection, or grouping of information maintained by an agency that contains an individual's name or other identifying information. A record, for example, could include information on education, financial transactions, or medical history. Under the Privacy Act, federal agencies must inform the public when they create a new system of records or revise an existing system. This is done through publication in the *Federal Register*. A new system of records is announced when an agency wishes to collect new data. Sixty-two of HCFA's 81 systems of records relate directly to Medicare beneficiaries and include personally identifiable data on a Medicare beneficiary's enrollment and entitlement to benefits; demographic information such as age, race, ethnicity, and language preference; and diagnostic and treatment information. HCFA's systems of records contain information stored in electronic and paper forms.

The Privacy Act generally prohibits the disclosure of individuals' records without their consent. However, it allows the disclosure of information without an individual's consent under 12 circumstances called conditions of disclosure. One example is disclosure by a federal agency to its employees baseD on their need for the records to perform their duties. Another condition of disclosure allows an agency to establish routine uses under which information can be disclosed to a data requestor. One routine use, for example, could be disclosure to an individual or organization for a research project related to an agency objective, such as prevention of disease or disability in HCFA's case. To establish a routine use, the agency must determine that a use is compatible with the purposes for which the information was collected and they must publish the notice of the routine use in the *Federal Register.* While the Privacy Act permits agencies to disclose information, it does not require that they do so; they can, for example, determine that in a particular case, the individual's privacy interest outweighs the public interest in disclosure.

HCFA NEEDS PERSONALLY IDENTIFIABLE INFORMATION ON MEDICARE BENEFICIARIES

Personally identifiable information is essential to HCFA's day-to-day administration of the Medicare program. Of primary importance is the need of the agency and its contractors to use personally identifiable information on Medicare patients to pay approximately 900 million fee-for-service claims annually. HCFA also uses this information to determine the initial and ongoing eligibility of Medicare beneficiaries, determine risk-adjusted payments, make monthly payments to about 400 Medicare managed care plans, and track which managed care plans have been selected by over 6 million Medicare beneficiaries. HCFA and its contractors use beneficiary

claims data containing personally identifiable information to prevent fraud and abuse; administer the Medicare Secondary Payer program;[2] develop fee schedules and payment rates used in fee-for-service claims processing; review the access, appropriateness, and quality of care received by beneficiaries; and conduct research and demonstrations including the development and implementation of new health care payment approaches and financing policies.

HCFA Discloses Information About Beneficiaries for Authorized Purposes

In screening requests for identifiable information, HCFA determines whether disclosure is authorized by the Privacy Act. It also has different levels of review depending upon the type of organization making a request for information. HCFA's policy and practice is generally to limit disclosures to information needed to accomplish the requestor's purposes. However, we found weaknesses in its recordkeeping system for tracking and reporting on disclosures and its notices to beneficiaries that their information could be disclosed.

HCFA Screens Requests for Personally Identifiable Information

In making decisions about whether to disclose information, HCFA's primary criterion is whether the disclosure is permitted under a routine use or one of the 11 other Privacy Act conditions of disclosure. HCFA can disclose information under routine uses to publicly and privately funded researchers and to public agencies such as the Agency for Health Care Policy and Research for health services research projects; to qualified state agencies for the purposes of determining, evaluating, or assessing cost effectiveness or quality of health care services provided in a state; and to insurers, underwriters, employers who self-insure, and others for coordination of benefits with the Medicare Secondary Payer program.

When deciding whether to disclose personally identifiable information, HCFA has different levels of review depending on the type of organization making a request for information. According to HCFA policy, HCFA employees and claims administration contractors are provided access to personally identifiable information only when they require such information to perform their official duties. Other federal agencies and organizations, such as state governments and law enforcement agencies seeking information on Medicare beneficiaries, must submit documentation, such as a signed data use agreement that indicates their acceptance of the confidentiality requirements of the Privacy Act and HCFA's data use policies and procedures. These policies and procedures include a requirement that the data user will not publish or release information that could allow deduction of a beneficiary's identity. When reviewing documentation from requestors, HCFA determines whether the disclosure, is permitted under a routine use for a system of records or other condition of disclosure, as allowed by the Privacy Act. In screening requests from outside researchers, HCFA also requires the submission of a detailed study protocol. Further, researchers must receive approval from the HCFA Administrator when they request the names and addresses of Medicare beneficiaries they intend to contact to collect new data.

HCFA Generally Limits Disclosures to Information Needed to Accomplish Purposes

HCFA officials told us their practice is to disclose the least amount of personally identifiable information that will accomplish the purpose of the individual or organization making the request. HCFA generally provides one of three types of data files—public-use files, beneficiary-encrypted files, and files which contain explicitly identifiable information. Public-use files are stripped of identifying information on beneficiaries and usually are summarized data. Beneficiary-encrypted files are data sets in which HCFA has encoded or removed the health insurance claim number, date of service, beneficiary name, or beneficiary zip code. Explicitly identifiable files contain such information as beneficiary names, addresses, and health insurance claim numbers. HCFA officials said they direct requestors whenever possible to either public use files or to beneficiary-encrypted files rather than to the files containing more identifiable beneficiary information. However, when HCFA does disclose data files with personally identifiable information, it generally does not customize them for the specific purpose of reducing the amount of information dis-

[2] The Medicare Secondary Payer provision limits payment under Medicare for otherwise covered items or services if that payment has been made or can be reasonably expected to be made from another source such as under a workmen's compensation law, automobile or liability insurance policy, or certain health plans. In such cases, Medicare payments for items or services are conditional payments and Medicare is entitled to reimbursement from the other sources for the full amount of Medicare payments.

closed. HCFA officials told us that to do so would be a resource-intensive process; however, they are now developing software that will permit them to more easily customize data elements in the future.

HCFA's Recordkeeping System for Tracking and Reporting Has Weaknesses

Although Medicare beneficiaries have the right under the Privacy Act to ask for and receive an accounting of disclosures of their personally identifiable information and to examine or amend their individual records, HCFA's recordkeeping system is incapable of readily providing an accounting of disclosures to beneficiaries. The Act requires that the accounting include information on the nature and purpose of the disclosure and the name and address of the person or organization to whom the disclosure was made. HCFA officials told us that the agency's computerized system for tracking disclosures cannot easily generate information for an individual beneficiary on disclosures made from HCFA's system of records. Weaknesses in HCFA's recordkeeping system also affect its ability to report on its Privacy Act activities to oversight agencies such as OMB.

HCFA officials also told us that they are working on improving their recordkeeping system to better account for disclosures of personally identifiable information made by the agency. HCFA officials said that, as directed by OMB, they have begun reviewing their recordkeeping for Privacy Act activities. In January 1999, OMB released guidance based on a May 14, 1998, Presidential memorandum directing each agency to review its information practices to ensure compliance with the Privacy Act. HCFA has begun to address OMB guidance and officials told us that they are reviewing routine uses that allow disclosure of Medicare beneficiaries' information. In May 1999, HCFA established an executive-level Beneficiary Confidentiality Board to review strategic confidentiality issues including HCFA's policies and procedures for disclosing personally identifiable information.

Weaknesses in Notifications to Beneficiaries That Their Information Could be Disclosed

The Privacy Act requires federal agencies to permit an individual to find out what records pertaining to him or her are collected, maintained, used, or disseminated by the agencies. The Act requires an agency to notify individuals of the following when it collects information: (1) the authority under which the agency is collecting the information, (2) the principal purpose for the information, (3) routine uses that may be made of the information, and (4) whether the individual is required to supply the information and the effects on the individual of not providing it.

HCFA officials told us they use more than a dozen different Privacy Act notifications when collecting information from beneficiaries. Individuals' first exposure to a Medicare-related Privacy Act notice is usually at the time of their application for Social Security retirement benefits, when they are provided with a multi-page Privacy Act notice. Approved Social Security retirement benefit applicants are automatically enrolled in Medicare at age 65. Beneficiaries should receive other Privacy Act notifications whenever HCFA collects information about them—for example, if they separately enroll in Supplemental Medical Insurance (Medicare Part B), receive medical care, or participate in a survey or a demonstration project.[3]

While some of the HCFA Privacy Act notification forms we reviewed contain the required information, we found that others do not tell beneficiaries the purposes for which their information may be disclosed outside of HCFA, or they do so in an unclear fashion. For example, a form for beneficiaries receiving services in skilled nursing facilities provided the required information, but the Privacy Act notice for Medicare Part B enrollment did not identify the routine uses that would be made of the beneficiary's information and provided only a vague reference to the *Federal Register* as a source for such information. We found similar problems in a form used to collect information on end-stage renal disease beneficiaries.

INADEQUATE HCFA SAFEGUARDS COULD COMPROMISE CONFIDENTIALITY

Although the procedures specified in HCFA's systems security manual generally adhere to OMB's guidance for safeguarding electronic information, HHS's OIG has identified serious control weaknesses with HCFA's safeguarding of confidential information.[4] OIG's audits of fiscal years 1997 and 1998 financial statements identi-

[3] Medicare Part B helps pay for doctors, outpatient hospital care, and other medical services such as physical and occupational therapy.

[4] HHS/OIG, *Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1996* (CIN: A–17–95–00096, July 17, 1997); HHS/OIG, *Report on the Fi-*

Continued

fied a variety of problems with HCFA's safeguards for electronic information at HCFA's central office and for selected Medicare claims administration contractors. The OIG reported the need for HCFA to implement an overall security structure and discussed weaknesses in the following areas: computer access controls (techniques to ensure that only authorized persons access the computer system), segregation of duties (the division of steps among different individuals to reduce the risk that a single individual could compromise security), and service continuity (the ability to recover from a security violation and provide service sufficient to meet the minimal needs of users of the system). The OIG also reported problems with controls over operating system software integrity and application development and change controls. However, HCFA has reported few complaints of potential Privacy Act violations.

When the OIG conducted work at 12 Medicare contractors for its fiscal year 1998 audit, auditors were able to penetrate security and obtain access to sensitive Medicare data at 5 of them. The auditors' ability to do so without using their formal access privileges is of particular concern because unauthorized users can exploit this security weakness in several ways, and compromise confidential medical data.

Agency officials told us they are in the process of taking action to correct the weaknesses identified by OIG. However, HCFA's ability to make progress is currently affected by the agency's efforts to address computer requirements for the year 2000 so that there will be no interruption of services and claims payments. HCFA, consistent with priorities established by OMB, has a moratorium on software and hardware changes until it is compliant with year 2000 computer requirements. OIG will evaluate the effectiveness of any corrective actions that HCFA is able to implement during its fiscal year 1999 financial statement audit.

HCFA Does Not Systematically Monitor How Organizations Protect the Confidentiality of Medicare Data

Although HCFA has a process for monitoring systems security at its claims administration contractors, agency officials told us that competing demands and resource constraints have prevented them from monitoring whether these organizations follow OMB guidance for protecting the confidentiality of information. HCFA officials told us that, other than OIG reviews, there were no explicit on-site reviews of contractor's security protections in fiscal years 1997 and 1998 because of resource constraints and the assignment of staff to assess contractor year 2000 computer requirements. However, HCFA did initiate reviews of network security in 1998 for 12 Medicare contracts at 4 of its 60 claims processing contractors.

In addition, HCFA officials told us that they do not have a system for monitoring whether organizations outside of HCFA have established safeguards for personally identifiable information received from the agency. When organizations sign data use agreements with HCFA, they agree to establish appropriate administrative, technical, and physical safeguards, providing a level and scope of security that is not less than the level and scope established by OMB. Data use agreements also include requirements that those receiving information from HCFA use the data only for their HCFA-approved purpose and that the data be returned to HCFA or destroyed upon completion of the project. HCFA does not systematically monitor how the data are being used. Although the agency follows up on expired data use agreements, HCFA currently has a backlog of about 1,400 expired agreements. It expects to reduce the backlog by one-half by September 30, 1999.

HCFA's failure to monitor contractors and others who use personally identifiable Medicare information hampers HCFA's ability to prevent the occurrence of problems and to provide timely identification and corrective action for those that have occurred.

Few Complaints of Privacy Act Violations Reported

The agency identified 7 complaints of potential violations of the Privacy Act it has received and resolved in the past 4 years. Six complaints involved contractors conducting research for HCFA, health data organizations, and individual researchers; the seventh complaint was made by a Medicare beneficiary's attorney. The first six complaints were raised by similar organizations or other researchers and involved posting of potentially identifiable Medicare billing information on an Internet website, using and publishing data in a second research project without authoriza-

---

nancial Statement Audit of the Health Care Financing Administration for Fiscal Year 1997 (CIN: A–17–97–00097, Apr. 24, 1998); HHS/OIG, *Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1998* (CIN: A–17–98–00098, Feb. 26, 1999). See also *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD–98–92, Sept. 23, 1998).

tion from HCFA, and offering to share Medicare files at a national research conference. In the first six cases, HCFA provided direction on Privacy Act requirements to those involved. In the seventh case, HCFA provided the beneficiary's attorney with a letter addressing the issues raised.

HCFA reported only one internal disciplinary action within the past 5 years relating to violations of HCFA's confidentiality policies. This incident involved an agency employee who was accessing beneficiary files more frequently than appeared necessary for performing his job. The employee admitted to looking at files of famous people. He was placed on administrative leave and later signed an affidavit stating that the files had not been sold or shared with other persons; accordingly, he was allowed to resign.

SOME STATES RESTRICT DISCLOSURE OF SENSITIVE CONFIDENTIAL INFORMATION

In its oversight of the Medicare program, HCFA necessarily deals with beneficiaries and providers from every state. Although states have laws governing the confidentiality of health information, these laws vary significantly, resulting in what has been called a patchwork system of protections. For example, in Florida, mental health records are confidential and may be disclosed only under limited circumstances.

Conflicts between HCFA and the states involving medical record disclosures have been minimal, according to HCFA officials, and HCFA officials believe its administration of the Medicare program has not been hindered because all states permit release of information for health care treatment and payment. If a state law prohibited disclosure of information to HCFA that was critical for these purposes, and a federal statute required such disclosure, HCFA officials told us that the agency would rely on the Supremacy Clause of the U.S. Constitution and its express statutory authority.[5]

HCFA officials told us that if information is not critical to HCFA operations, HCFA's policy is to respect and abide by state laws that provide greater health records protection than would otherwise be required by federal law or regulation. For example, when California and Washington notified HCFA that laws in their states did not authorize the disclosure of diagnostic information related to the human immunodeficiency virus (HIV), acquired immunodeficiency syndrome (AIDS) and sexually transmitted diseases (STD), HCFA changed the system used to collect and analyze certain nursing home information by allowing the states to withhold diagnostic information collected about HIV/AIDS and STDs for their nursing home patients.[6] HCFA told us that 15 states have exercised this option by blanking out identifiable codes for HIV/AIDs or STDs before submitting the requisite information to HCFA. According to HCFA officials, the deletion of diagnostic information collected about HIV/AIDS and STDs for nursing home patients generally has not affected its operations. However, HCFA officials told us that the agency will require diagnostic information as it refines its new prospective payment system for skilled nursing facilities as well as its other payment systems and may, therefore, need to change its policy of allowing states to withhold information.

Restricting HCFA from receiving uniform health information across the country could adversely affect internal operations such as rate-setting and monitoring for quality assurance. It could also affect the ability of analysts in HCFA, other federal agencies, and non-governmental organizations to conduct policy analysis and health services research because of the difficulty in complying with varying state laws. If the same data elements and health information were not available from all states, HCFA's ability to conduct research and analysis to improve Medicare policies might be compromised.

CONCLUSIONS AND RECOMMENDATIONS

In its role as administrator and overseer of the nation's Medicare program, HCFA must collect and maintain personally identifiable information on millions of beneficiaries to effectively operate and manage the program. As a steward of confidential information, HCFA must balance its need to effectively manage the Medicare pro-

---

[5] U.S. Const. Art. VI, cl.2. The Supreme Court has construed the Supremacy Clause of the U.S. Constitution to hold that federal law preempts state law where, for example: (1) the state law directly conflicts with federal law, (2) the federal legislative scheme leaves no room for state regulation, or (3) the state statute frustrates or conflicts with the purposes of the federal law.

[6] The information is used by HCFA to track changes in health and functional status of nursing home residents. The information system is known as the National Minimum Data Set (Resident Assessment Instrument) repository.

gram with the privacy concerns of its beneficiaries. HCFA must protect beneficiaries' health information from inappropriate or inadvertent disclosures.

We found that HCFA's policies and practices are generally consistent with Privacy Act protections. However, we also found that the agency needs to do a better job implementing and enforcing certain protections. As the HHS OIG has reported, HCFA continues to have vulnerabilities in its information management systems. In addition, HCFA has not consistently monitored its claims administration contractors' safeguards for protecting confidential information. We recognize that HCFA, consistent with priorities set forth by OMB, has focused its resources on ensuring that the agency and its contractors are compliant with year 2000 computer requirements. Nonetheless, we believe that reducing the vulnerabilities in its information systems and increasing its monitoring of contractors are important concerns that HCFA must address in the coming year.

HCFA also needs to better implement other aspects of its confidentiality policies and practices. The agency does not always fully and clearly inform beneficiaries that their information may be disclosed. It also lacks the ability to readily provide beneficiaries with an accounting of disclosures. In addition, HCFA does not have a formal system for monitoring the confidentiality protections of organizations to which it discloses personally identifiable information. As a result, HCFA is unable to systematically reduce the likelihood of inappropriate use of the data or identify instances of such misuse.

Although few complaints about Privacy Act violations have been made to date, we believe that the weaknesses we and others have identified potentially compromise the confidentiality of health information on Medicare beneficiaries. However, HCFA has begun some important initiatives that appear promising and could improve its protection of Medicare beneficiary health information. These include the creation of a new beneficiary confidentiality board and actions taken in response to OMB guidance for agencies to reevaluate the circumstances under which they disclose information.

Our report makes recommendations to the HCFA Administrator to improve HCFA's protection of the confidentiality of personally identifiable information on Medicare beneficiaries. In summary, we recommend that HCFA correct the vulnerabilities identified in its information management systems by OIG, systematically monitor contractors' safeguards for protecting confidential information; develop a system to routinely monitor other organizations that have received personally identifiable information on Medicare beneficiaries; ensure that all agency Privacy Act notifications contain the information required by the Act in a form that is clear and informative to beneficiaries, and implement a system that would permit HCFA to respond in a timely fashion to beneficiary inquiries about disclosure of their information outside HCFA as well as to provide information on Privacy Act activities to OMB and others.

Mr. Chairman, this concludes my prepared statement. I would be happy to answer any questions you or the Subcommittee Members may have.

GAO Contacts and Acknowledgements

For future contacts regarding this testimony, please call Leslie G. Aronovitz at (312) 220–7600 or Bruce D. Layton at (202) 512–6837. Key contributors to this testimony include Nancy Donovan, Bonnie Brown, Nila Garces-Osorio, Barry Bedrick, and Julian Klazkin.

Related GAO Products

Medicare: Improvements Needed to Enhance Protection of Confidential Health Information (GAO/HEHS–99–140, July 20, 1999).

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T–AIMD–99–214, June 22, 1999).

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T–AIMD–99–160, Apr. 27, 1999).

Financial Audit: 1998 Financial Report of the United States Government (GAO/AIMD–99–130, Mar. 31, 1999).

Auditing the Nation's Finances: Fiscal Year 1998 Results Highlight Major Issues Needing Resolution (GAO/T–AIMD–99–131, Mar. 31, 1999).

Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Is Limited (GAO/HEHS–99–55, Feb. 24, 1999).

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid

Major Disruptions (GAO/T–AIMD–50, Jan. 20, 1999).
Major Management Challenges and Program Risks: Department of Health and Human Services (GAO/OGC–99–7, Jan. 1999).
Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD–98–284, Sept. 28, 1998).
Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD–98–92, Sept. 23, 1998).

Chairman THOMAS. Thank you very much.

Dr. Hamburg, it has been a source of frustration for many of us that the administration has failed almost in every instance to meet a date that was prescribed for it in law and to provide information or structure dealing with the BBA in terms of prospective payment structures of the rest. So that source of frustration may indeed be finally useful in your announcing that the administration plans to produce its document on a particular timetable, and I feel comfortable that that timetable will not be carried out. This is the first time I feel good about the Administration not making a timetable.

Ms. Aronovitz, in the GAO report, on page 6, you indicate that HCFA relies on, under current conditions, the disclosure structure provided for in the Privacy Act dealing with release of information to outside researchers and other entities; and you also mentioned in your testimony and on page 14 and 15 you note that HCFA's current recordkeeping system makes it almost impossible for someone to go back and determine where all someone's data was sent. And I know Dr. Hamburg mentioned an HMO in terms of disclosing this information, and I appreciate your pointing out this problem.

However, in looking at GAO information the way you have it structured, Ms. Aronovitz, I don't see much of an indication of the number of these disclosures. You talk about 1,400 expired data use agreements. Now, the assumption is that covers a kind of an understanding of what information is going to be provided and what you are going to do with it, but those are expired data use agreements, 1,400 of them. How many are out there that are not expired? That would be one of the questions. How many over a time period, 1 year, 5 years, has there been in terms of agreements in which information has been moved? Do we have any indication of the total number of agreements?

Ms. ARONOVITZ. No. It is actually quite a complicated accounting process. When you think of the Privacy Act, we usually think of a system of records, and that is the kind of denominator which we use to try to figure out disclosures. We could not get an accounting of the total number of times data that were in a particular system of records were disclosed to an outside requester.

Chairman THOMAS. Is HCFA required to report Privacy Act information activity and to whom is it supposed to report this?

Ms. ARONOVITZ. HCFA has two obligations. The first is to the beneficiary, when the beneficiary asks for an accounting of disclosures. We believe that, right now, a beneficiary would probably have to wait for a while, because HCFA could not readily provide that information. HCFA also must provide certain types of information through HHS to OMB the information to be provided to OMB

concerns the number of beneficiaries who have asked to access their own records.

Chairman THOMAS. So the only information under the Privacy Act that is kind of held responsible for telling folk you are doing it is either to the individuals or the number of individuals information? Who are these entities, for example, on the 1,400 expired data use? Who would these agreements be with, typically? I know they are expired, but it would be an indication of who they would be with if they were alive.

Ms. ARONOVITZ. Data use agreements are used for a variety of requesters of information from HCFA. They would be almost everyone outside of HCFA itself.

Chairman THOMAS. Who is everyone? Are these entities?

Mr. HASH. It would be HCFA, it would be researchers that HCFA is sponsoring, research or non-HCFA sponsored researchers. It could also be States or other Federal agencies.

Chairman THOMAS. And there is no requirement that they list or include who it is that they have transmitted this information to on a Privacy Act report to OMB?

Mr. HASH. No, there is no requirement for disclosures to third parties in the OMB. It is only to the number of times a beneficiary has asked to access its own information.

Chairman THOMAS. Thank you.

Do you volunteer this information anyway or do you follow strictly the Privacy Act?

Mr. HASH. Mr. Chairman, we have been trying to follow the Privacy Act. We have actually to my knowledge not recorded any requests from beneficiaries for the information that Ms. Aronovitz——.

Chairman THOMAS. I am asking the question the other way. Do you keep track of who it is, the entity that you enter into these agreements with and to which you release personally identifiable information?

Mr. HASH. We do.

Chairman THOMAS. Then tell me how many you have entered into over the last 1 year, 5 years.

Mr. HASH. I will have to get you that for the record, Mr. Chairman.

Chairman THOMAS. Do you believe you can get it for the record?

Mr. HASH. I believe we can. I believe we could determine the number of data use agreements that we have.

[The following was subsequently received:]

Within the last year 1,911 data use agreements were initiated. Of these, 1,261 involve identifiable data and 650 involve encrypted data. Within the last five years 5,167 data use agreements were initiated. Of these, 3,950 involve identifiable data and 1,217 involve encrypted data.

Chairman THOMAS. OK. My problem is, if you can do that, Ms. Aronovitz, my understanding is you interviewed HCFA folk, and did you ask that question of them?

Ms. ARONOVITZ. The data use agreement is between the researcher and HCFA. HCFA needs to be able to better account for

specifically what records they are disclosing on a particular beneficiary.

Chairman THOMAS. So we don't even know what information is transmitted to these individuals? Or we do, but we can't recall it after it is done?

Ms. ARONOVITZ. The details are kept in paper records filed by the requester's name, not by an individual beneficiary or by a system of records.

Chairman THOMAS. Now I also noted in the GAO report that HCFA indicated that what they did was follow the tail of the comet, that is, they would review on the Internet, read materials to see if any of this information was out there. And it just kind of concerns me that they don't look at the comet, they look at the tail of the comet, so it is already out there before their detection structure would function; is that correct?

Ms. ARONOVITZ. Yes. We think they need to do a much better job doing more proactive monitoring of entities that they provide information to, making sure that they are following their data use agreements and, in fact, complying with the provisions of those agreements.

Chairman THOMAS. So, based upon Dr. Hamburg's testimony, I could very comfortably ask her who has HCFA released individual information out of HCFA to, and she probably wouldn't be able to tell me who she released it to. Probably just as important, she wouldn't be able to tell me what it was that was released, unless of course it appeared on the Internet being misused if your monitoring is 100 percent accurate after the fact. Is that a reasonable statement of what we have got right now with individualized records being sent out of HCFA to researchers and other entities?

Ms. ARONOVITZ. I think it is reasonable. We would have to say that it would take quite a lot of effort, for HCFA to get that information.

Chairman THOMAS. Mike, you want to respond?

Mr. HASH. Mr. Chairman, what I would like to say is that we, in fact, do I think have, as I mentioned a moment ago, the records, the data use agreements that we have entered into.

Chairman THOMAS. And you know what it is that has been transmitted under this agreement? You have a record of that?

Mr. HASH. We do. We do. What would take a greater effort that was referred to was the identification specifically on a beneficiary by beneficiary basis, what various systems of record information was transmitted. It could be done, but because we maintain our records on the basis of the data use agreement, you would have to go in and manually identify the individuals that were included in that data use agreement, but we know what we gave and to whom we gave it.

Chairman THOMAS. You know what you gave.

Mr. HASH. Correct.

Chairman THOMAS. Including personalized medical record information from an individual.

Mr. HASH. We know the systems of records that include personally identified information that we made available to a user under a data use agreement.

Chairman THOMAS. And do you know they honored that use agreement?

Mr. HASH. I believe except for the monitoring activity we need to put into place stronger oversight of exactly whether all of the users in these data use agreements are complying with the requirements of the Privacy Act.

Chairman THOMAS. I appreciate the answer. The question was, do you know if they are living up to the agreement?

Mr. HASH. Not in every case, Mr. Chairman.

Chairman THOMAS. And have you found some since, not in every case, there are some who are not?

Mr. HASH. Very few.

Chairman THOMAS. OK. What do you do with the few that you find?

Mr. HASH. In the cases where people have violated the Privacy Act, we have of course withdrawn, canceled their——.

Chairman THOMAS. Don't you want to modify the statement to say that in those instances when we are aware they have violated the agreement?

Mr. HASH. In those instances, where we believe there has been a violation of the Privacy Act by one of our——.

Chairman THOMAS. No, that you are able to determine—see, what you did was just go from a statement in which you don't do a very good job of keeping track of it and you have discovered some violations——.

Mr. HASH. Mr. Chairman, I think we do a good job of keeping track of it. What we don't do as good a job of as we should is in oversight with these users to make sure that, once they get the data, they are in fact actually complying with the requirements of the Privacy Act.

Chairman THOMAS. And how many agreements are there today in effect?

Mr. HASH. I will be happy to try to supply that to you for the record. I don't have it with me, Mr. Chairman.

[The following was subsequently received:]

As of July 21, 1999, there are 4,377 data use agreements in effect. Of these, 2,924 involve identifiable data and 1,453 involve encrypted data. The majority are with government agencies and researchers under contract to do work for the government; only 515 are not with Federal or State agencies or researchers under contract to such agencies.

Chairman THOMAS. OK. Now, GAO has identified, you know, many uses that HCFA has with the individually identified information. You got to do a lot of stuff. You have got payment activities that you have to deal with that data, claims processing. You do some utilization review. You got secondary payment enforcement, eligibility determinations. What else? Integrity activities, peer review, quality assurance.

Mr. HASH. Yes, sir.

Chairman THOMAS. What else? I mean, some research——.

Mr. HASH. Yes, sir, for purposes of improving either our payment policies or our quality improvement strategies.

Chairman THOMAS. Yes. Would you classify the surveying of individual claims files in order to determine something like, say, the relative mammography rates of seniors in the traditional fee for Medicare service program to be a quality assurance activity?

Mr. HASH. I believe we would, Mr. Chairman.

Chairman THOMAS. How about peer review and credentialing activities?

Mr. HASH. If you mean by that organized systems of care, Mr. Chairman?

Chairman THOMAS. Yes, trying to take a look at who does what in the credentialing area as a kind of, in my opinion, a quality assurance procedure. Would you classify that, the credentialing, the review of the ability to live up to the agreement that was made for credentialing purposes, quality assurance?

Mr. HASH. The situation that that suggests to me is that the—only one area wherein we review applications of private health plans and want to contract with Medicare and we look to those private health plans to provide us information about their credentialing procedures for health care professionals who are going to serve our enrollees.

Chairman THOMAS. OK. Let me give you an example. The President's recent proposal said that he is interested in moving toward a PPO, preferred provider organization structure, and my assumption is you are going to have to do some additional monitoring and perhaps some credentialing in that regard. Would that be a quality assurance activity?

Mr. HASH. Well, we have been thinking about two approaches to that, Mr. Chairman. One would be to contract with existing PPO organizations that are already out there; and in that case, obviously, we would be interested in assurances that they do have some criteria for determining who gets admitted to their PPO. We had not really anticipated, at least initially, that we would be forming under that proposal our own PPOs.

Chairman THOMAS. But it doesn't preclude that.

Mr. HASH. It does not.

Chairman THOMAS. And this line of questioning was in part to establish that, obviously, health information is sensitive, it is important, but there are truly legitimate reasons beyond treatment and payment that you need to utilize this kind of data if for no other reason quality assurance but certainly in terms of best practices and other activities I think are important.

My real concern as we move forward in this is that we take a look at where we are philosophically, where we may want to be for public health purposes and, in fact, providing statistical data to be able to assist in improving individual health care and look at what is happening at the State level and the ability of the Federal Government, notwithstanding the fact it is a sovereign, to make sure all legitimate health entities have the ability to do the same thing. And I am concerned about the administration's position that they are less concerned about what is happening at the State level because of the sovereign position and HCFA's ability to collect information. But the formation of a confidentiality structure which provides for research collection needs to be looked at from a Federal

perspective, not just a government but a national perspective for the data. Is there any reaction to that?

Dr. HAMBURG. Well, I think that the Secretary's recommendations definitely acknowledge the important point you are making and identify research as an important area of activity for disclosure of information, public health concerns, quality of care and certain emergency situations as well.

Chairman THOMAS. The gentleman from Wisconsin has already had his position violated by the Secretary's concerns. So since we have blown through his concerns, my concerns are this. I understand the concept of a Federal floor and allowing States to go beyond that. If we are dealing with things like clean water, clean air, it doesn't make sense to me if you are dealing with the collection of data to say there could be a Federal floor but States can impose more stringent data in particular areas. We may want to carve out other areas completely.

I do not understand—and this is kind of a bizarre relationship to me—a Republican advocating Federal preemption in an area in which that folk at a cocktail party would think that would be understanding the importance of the collection of data for very fundamental and critical reasons in the private sector as well as in the public sector. And this is an area I think we need to resolve because I do not understand how, in the collection of data for useful purposes, the administration can comfortably say we will establish a floor and if the State wants to go beyond that, that is OK with us. How ever in the world you have an accurate, universally reliable data collection system with that basic organizing concept doesn't make sense to me, and I look forward to continuing to work with you.

The gentleman from Wisconsin wishes to inquire?

Mr. KLECZKA. Thank you, Chairman Thomas.

I don't believe the Secretary did violate my preamble for privacy, because I never said it was an absolute right. I said as the owner of those records I think I should have the right to express my desire for privacy. Throughout the discussion of the use of these records for research and for collection of data I think we should consider, de-identifying the records. I think, for billing purposes my name and data might have to be attached to it, but for a lot of stuff we can de-identify the medical record and let the research or whatever go forward.

Mr. Hash, first let me ask a question we are all wondering and I guess everyone is kind of embarrassed to ask, how is the mother to be?

Mr. HASH. I am glad you asked that. I just talked to her today, and she is expected to deliver at any moment, so she is very near the end of her odyssey and very excited about the next phase of her life.

Mr. KLECZKA. Well, we wish her well and the baby and the father.

Let me ask one question. You indicated that HCFA has just approved the creation of a Beneficiary Confidentiality Board, which I assume is going to be akin to the Independent Review Boards that States have and some individual private organizations have.

What do you envision the responsibility of this confidentiality board to be?

Mr. HASH. Mr. Kleczka, I am glad you asked, because we felt we needed a high-level organization within HCFA that pulled together the leadership of the agency to focus on the strategic questions about the kind of information that needed to be collected to operate our programs, as well as the protections that need to be in place to ensure patient and individual confidentiality. And the mission of this new Beneficiary Confidentiality Board is to develop procedures and policies that will govern our decisions about the collection of information on the front end, as well as our requirements for data users and, in fact, our policies and procedures for overseeing, as I mentioned to Chairman Thomas, compliance with these procedures by anyone with whom we enter into a data use agreement.

We are also anxious that this board be an opportunity to examine the existing systems of records that we have to determine whether they are properly secured, whether we in fact, in another critical area, are making adequate notices available to our beneficiaries so that in plain language they know under what authority we are collecting the information and specifically to what uses it could be put.

So these are the range of broad questions that we expect this board to address; and, as I say, not only does it involve our computer and information systems people, but it is actually housed, for staffing purposes, in our Center for Beneficiary Services to focus attention that this is all about protecting the interests of our beneficiaries.

Mr. KLECZKA. With the thousands of contractors that you enter into agreements with across the country, have you seen any violations of the beneficiaries' medical records by contractors either through unauthorized viewing or sale of information?

Mr. HASH. We are not aware of any serious violations. We think there have been instances in which the procedures for gaining access to personally identifiable information may have been breached because individuals who were not authorized by the nature of their work to have access may have been given access. When we have learned of that, we have, you know, revoked their access privileges and taken steps to tighten up on the approval of access, but, to my knowledge, we do not have any cases where the information has been sold or publicly disclosed.

Mr. KLECZKA. OK. In how many instances do you recall having a problem with contractors with regard to unauthorized access?

Mr. HASH. How many instances?

Mr. KLECZKA. How many instances? Do you have any numbers?

Mr. HASH. I think it is very few over the last 5 or 6 years. We looked back, and I think we only found one or two altogether.

Mr. KLECZKA. OK. When you deal with a patient's privacy and the records that you are responsible for you comply with Federal Privacy Act, but you also defer to State law; is that accurate?

Mr. HASH. We generally do respect State laws. For the most part, what we have found is that State laws do recognize the kinds of needs that we have for personally identified information in their own laws, for example, data for payment purposes, data for fraud and abuse purposes and law enforcement, and data for quality as-

surance. These are typically treatment, payment and health care operations exceptions that are found in State privacy laws, and those laws have allowed us to continue to have access to the data we need to operate our programs.

Mr. KLECZKA. OK. I will get back to Ms. Hamburg on the second round with some preemption questions. Thank you.

Chairman THOMAS. Gentlewoman from Connecticut wishes to inquire?

Mrs. JOHNSON of Connecticut. I thank you for your testimony today.

I want to talk a little bit more about this patient opt-out power as well and particularly how it interfaces with the floor proposal. If a patient has the right to opt-out, and I am very sympathetic to the opt-out provision but I want to understand more clearly how it works, could a Medicare beneficiary elect to withhold the fact that they had had a certain diagnosis?

Mr. HASH. I think you are addressing that to me, Mrs. Johnson.

Mrs. JOHNSON of Connecticut. Well, whoever is best suited to answer it.

In other words, could they elect to withhold this information from the carrier, you know, from the payor? I want to know how far their election rights go. The doctor knows it clearly. Now if they can elect to withhold this information, I might want to do exactly what my friend did with his dentist. I might like to elect to withhold that I was diagnosed with shingles for a fear that people would fear that I was hyper responsive to stress-related illnesses. So, you know, how much could they withhold actually from the carrier?

Mr. HASH. Well, the requirements in the Medicare Program are really to submit a claim to us that provides sufficient information on the claim form for us to determine if the individual is eligible, that the service provided was covered, and that is the basic information that comes in on a claim form. And if a claim form was submitted to us without the diagnostic information or without the identification of the individual or their health insurance number, then our contractor would be unable to process that claim.

Mrs. JOHNSON of Connecticut. OK. Then in terms—because I want to go through a sort of series of these—in terms of program activities that HCFA is responsible for, could an individual elect not to let HCFA use specific data in research and development of new payment methodologies? In other words, I could see that they would have to submit the information so there would be payment, but could they prevent you from having access to that information for your own internal research and policy development?

Mr. HASH. As I understand it, Mrs. Johnson, under our current notices, and the authorizations that we seek from our beneficiaries when they enroll in Medicare, allow us to make the judgment about the use of their personally identified information for purposes that may involve research related to the improvement of the payments in the program or to quality oversight or to fraud and abuse, those kinds of activities.

Mrs. JOHNSON of Connecticut. How specific is your requirement to inform consumers and to ask for their permission? Because in the next 5 years there are people who are going to get much more

sensitive to this whole issue and are going to be making different decisions. So do you inform them they have a right to withhold information and will there be subcategories that you have a right to withhold your information from researchers, you have a right to withhold information from whomever?

Mr. HASH. That is not the substance of our notices that we give under the Privacy Act now. They do not have the option to sublimit the use of the data for the kinds of examples that you were using.

Mrs. JOHNSON of Connecticut. So when they say disclose or not disclose, do they know to whom the information may be disclosed and to whom it may not be disclosed?

Mr. HASH. Of course they don't know specifically to whom it may be disclosed, but they do know that it may be disclosed for a series of purposes, and those purposes are indicated in the notice.

Mrs. JOHNSON of Connecticut. And if they indicate they don't want disclosure, do you interpret that to mean that you simply can't disclose to an outside contractor but you can disclose within your agency? Do you say that you can disclose to other Federal agencies but not to outside contractors?

Ms. ARONOVITZ. My understanding right now is that on a notice it is a blanket notification. We actually looked at some notices that say, if you do not sign this form, you will not be able to get benefits from Medicare.

Mrs. JOHNSON of Connecticut. That is not an opt-out to say if you don't sign disclosure you don't get benefits under Medicare. This is a sledgehammer.

Ms. ARONOVITZ. We don't consider that an opt-out.

Mrs. JOHNSON of Connecticut. Oh, I see.

Ms. ARONOVITZ. If there is an opt-out policy——.

Chairman THOMAS. It may be a literal opt-out, depending upon what options you need and medical service.

Ms. ARONOVITZ. Currently, we don't see HCFA having an opt-out policy.

Mr. HASH. To my knowledge, we do not.

Mrs. JOHNSON of Connecticut. I thought you were recommending an opt-out policy.

Mr. HASH. I am not aware of that, Mrs. Johnson.

Mrs. JOHNSON of Connecticut. My impression is that in your recommendations you are proposing an opt-out policy. So I kind of assumed from that, which I did not have the right to assume, that if you are recommending an opt-out policy you must already have one.

Mr. HASH. Perhaps this will be helpful, Mrs. Johnson. We do have a procedure where if a researcher wants to contact an individual about their participation in a survey or some kind of a research protocol that we first contact that individual by letter and indicate to them that they may elect not to participate in such an activity if they do not want to. And that is an area of patient choice, if you will, or opt-out that we do routinely apply if the research protocol involves contacting an individual directly and asking them for participation in a research protocol.

Ms. ARONOVITZ. There is another example that might be useful. Some of the notices that we looked at specifically said if you don't

sign this form you will not get Medicare benefits. The OASIS notification, which we think is an improvement over some of the other notices, does have language that specifically states there are no Federal requirements for home health agencies to refuse you services if you do not provide this information. However, it takes a little bit of fortitude to really understand what it says.

Mrs. JOHNSON of Connecticut. Sort of a backhanded way of saying that you can get the services even if you refuse to disclose.

Ms. ARONOVITZ. Right, in this particular case. So there could be instances where you would not lose your benefits.

Mrs. JOHNSON of Connecticut. So there is not currently any requirement that when you sign up for Medicare you have the right to sign a waiver that says you may not release my medical information.

Ms. ARONOVITZ. As far as we know, that is correct.

Mr. HASH. I believe that is correct. The authorization that beneficiaries sign when they enroll in Medicare is a broad authorization.

Mrs. JOHNSON of Connecticut. Thank you. I will pursue this later, but I think in the new world this is a very big issue. Thanks.

Chairman THOMAS. Gentleman from Minnesota wishes to inquire?

Mr. RAMSTAD. Thank you, Mr. Chairman. Thank you to today's witnesses.

As a former adjunct professor of constitutional law, the more I get into this area I am beginning to reach the conclusion that health care privacy is an oxymoron given the state of technology, and I am real concerned about the right to privacy, the zone of privacy as the Supreme Court has talked about, that we supposedly have through the first, fourth, fifth and 14th amendments to the Constitution.

And I don't understand, if I may address the first question to you, please, Mr. Hash, according to the GAO critique, the report, when HCFA discloses data files with personally identifiable information it doesn't customize them for the specific purpose of reducing the amount of information. Now, I thought this was departmental policy pursuant to the 1997 HHS recommendations on privacy, and does this mean that they are ignoring the issue of customizing the data you disclose?

Mr. HASH. I think maybe, and I will let Ms. Aronovitz speak to that, but I think what we mean by customization is that at HCFA when we review a request for personally identified information for a research purpose, we actually go through a kind of three-stage evaluation. We have what are called public use tapes which have a lot of aggregated data which do not identify individuals; and we see if, in fact, research can be conducted with a public use tape.

We have a second level of release of data that involves the encryption of identifying information. It is obviously conceivable that with that data set you could identify individuals, but it would be difficult.

But we then, last, only as a last resort do we actually release a data file with person-specific identifiers in it, and only then when we have made a determination that there is no other way to con-

duct the research and that the research is vital to a purpose of administering our program.

Ms. ARONOVITZ. I would agree with that. However, if HCFA decided that the only way to fulfill the research purpose was to provide personally identifiable information, it does not have the capacity to only provide the data elements that are absolutely necessary to fulfill the research purpose. At that point if HCFA felt that the researcher really only needed, let us say, five data elements from that file that is where customization would not occur.

Mr. RAMSTAD. And it is a question or an issue of capacity of the resources?

Ms. ARONOVITZ. That is correct.

Mr. RAMSTAD. To customize to that degree?

Ms. ARONOVITZ. HCFA has said it is developing software that in the future will enable it to do a much better job with customization, but right now it doesn't have the capability.

Mr. RAMSTAD. Just recently I was privy to a demonstration by a computer expert who accessed his file at Columbia Presbyterian or wherever, revealed psychiatric data, other very confidential, sensitive data. All I could think of was this is Kafkaesque. I mean it was very, very unnerving, to say the least, and it just seems to me that we need to, this session, this year, we need to come to a consensus on a bill and get this done sooner rather than later. Would all three of you agree on that?

Mr. HASH. Yes.

Ms. ARONOVITZ. Yes.

Mr. RAMSTAD. And then, finally, I want to ask Ms. Aronovitz a question just briefly in the remaining seconds I have. In your GAO report, you mention that HCFA has not done much to inform Medicare beneficiaries about their rights under the Privacy Act. Could you elaborate on your findings? I mean, it is disappointing when this Subcommittee did a lot of work pursuant to the Balanced Budget amendment to ensure that beneficiaries receive clear and complete information about the Medicare Program, and I was just disappointed to read that finding. I was just wondering if you could elaborate on that.

Ms. ARONOVITZ. As I said, the OASIS notification is an improvement over prior ones. HCFA said it uses about a dozen or so different types of notifications. When somebody signs up for Medicare and then when they participate in the demonstration or obtain health care, there would be a notification. The Privacy Act requires a notification that has four elements, and they are very straightforward. You have to tell the beneficiary your authority for collecting the information, the principal purposes you will use it for, all of the routine uses you will make of the information and also the effects on the beneficiary of not providing the information.

Well, first of all, we found that some of the forms HCFA uses didn't have all these elements and, therefore, were incomplete, in our judgment, in terms of providing information to the beneficiary. However, interestingly, the Privacy Act does not require HCFA anywhere on these notices to indicate that beneficiaries have a right to get an account of the disclosures that are made of their information. This type of information did not appear on any of these notices.

Mr. RAMSTAD. Well, I see my time has expired, but I appreciate the explanation. It only makes me wonder that perhaps that is the reason so few seniors have ever contacted HCFA to see their information or to see HCFA's accounting of the disclosures it makes. But I look forward to working with all three of you and others on re-establishing the right to privacy in this country. A lot of this is truly alarming, and I don't say that talking in hyperbolic tones. I am very concerned, and I am glad to see you nodding affirmatively you share that concern.

Thank you, Mr. Chairman.

Chairman THOMAS. I thank the gentleman.

I do believe that it is a contest between public and private rights, and there are significant public rights when it comes to health and the effect that a single individual may have on the public health, and these are sometimes competing rights, and society historically has indicated that in certain instances the public's right to know to deal with the public health problem can even transcend privacy rights. And we are going to try to deal with that in balancing it, not only in after-the-fact information but hopefully in a successful prior-to-the-fact management in a world in which it is far more complicated with computers but ironically enough also simpler in certain instances because of the ability to control the flow of data via electronic means.

Gentlewoman from Florida wishes to inquire?

Mrs. THURMAN. Thank you, Mr. Chairman, and it kind of goes to that question.

Ms. Aronovitz, when I was looking over your report—and, of course, it was basically to talk specifically about protecting beneficiaries' confidential health information, one of the things that struck me was that we talk about the security weaknesses but we also talk about the moratorium that OMB has placed on HCFA in securing or looking at any other kind of computer software. Is that something we should look at correcting to give them the tools that would be necessary to help them in this job?

Ms. ARONOVITZ. Actually, the moratorium seems to be very appropriate under the circumstances. We think, in our Y2K work, that HCFA is facing quite a high risk in the fact that it is so close to the end of the year. We understand that HCFA needs to focus its resources on its immediate responsibility continuing to be able to pay claims. Unfortunately, the moratorium had to occur because it was one way for HCFA to assure itself that its resources would be centered on that immediate problem.

However, we think that fixing the security systems for privacy issues is extraordinarily important also and should be addressed as soon as HCFA's systems have been tested and certified as Y2K compliant.

Mrs. THURMAN. And is that what OMB has indicated that, once that is done, that those resources would be immediately available for this particular issue, Mr. Hash?

Mr. HASH. Yes, Ms. Thurman, that is my understanding; and it is certainly our intention that, once we pass the Y2K period, that this issue of installing the appropriate architecture for information technology security is our highest priority with our contractors. Because it has been pointed out to us by the GAO and by others that

there are steps we can put into place, new systems, new technology that mitigate the possibility of breaches of those systems by unauthorized persons, but, you know, this is an area where the technology is racing ahead as fast as we can possibly think about keeping up with it, and I think our real challenge is to remain vigilant to the possibility that just when you think you may have a computer system that cannot be hacked into, somebody will undoubtedly be able to figure it out. But that doesn't relieve us of the responsibility of taking all the steps we can to put in the strongest security measures available.

Mrs. THURMAN. So you all are working on this problem somewhat consecutively with the Y2K? I mean, you are looking for those ways, vendors, people who could in fact put in this software?

Mr. HASH. We are. And, in fact, another aspect of this is holding our contractors more accountable to, in our evaluation of them, that they, in fact, have put into place the appropriate kinds of security protections that are necessary to protect this data. So we recognize, as I said to Chairman Thomas earlier, that we need to strengthen our oversight of those organizations that have access to this kind of information to prevent unauthorized disclosures.

Mrs. THURMAN. Thank you.

Chairman THOMAS. I thank the gentlewoman.

Gentleman from Michigan wishes to inquire?

Mr. CAMP. Thank you, Mr. Chairman.

I thank all three of you for testifying today.

Ms. Aronovitz, I have a question for you. In your testimony you note that there are different needs that HCFA has for individually identifiable information and that there are beneficial uses of that information but, also, that there are some problems in maintaining the security of that data, you know, particularly regarding some of the administrative procedures and managing this in the context of an information system. What do you think the implications would be for HCFA if they had to comply with 50 different State laws?

Ms. ARONOVITZ. I think that it would add a tremendous complexity to their work and a burden and cost that we can't estimate, but it could certainly create quite an additional burden for them.

Mr. CAMP. In addition, what if Medicare patients could selectively demand that certain criteria were not or data elements were not to be used for certain purposes? Administratively, what do you think the impact and also that that information couldn't be disclosed to certain employers or employees or contractors?

Ms. ARONOVITZ. I am not an expert on HCFA's or anyone's computer systems, but I certainly feel comfortable in saying that the point that HCFA is at right now, if somebody were to be very specific about the circumstance under which they wanted their information to be used, it would be impossible for HCFA to comply.

Mr. CAMP. Would you agree that the private sector providers would face the same administrative burdens if Federal law wasn't preemptive and in fact might even be worse because they wouldn't have the supremacy clause to ignore certain laws at their discretion like HCFA might have?

Ms. ARONOVITZ. It seems as though they would have the same burden.

On the other hand, we didn't really look at how they are coping right now, and ostensibly there are companies that work in more than one State or all 50 and somehow seem to figure out how to get along, but we really don't know enough about how they are doing it or the extent to which that burden could convince some of them not to do commerce in the States.

Mr. CAMP. Thank you very much.

Mr. Hash.

Mr. HASH. May I comment?

Mr. CAMP. Yes.

Mr. HASH. I think there are a couple of observations I would like to make, and that is, they are—first, it is difficult to determine in advance exactly how States might in the future design privacy laws. And as I mentioned at the outset, our experience today has been that States have been generally sensitive to the kinds of issues that are necessary from our point of view to operate our programs and to meet our fiduciary responsibilities as well as our quality oversight responsibilities.

And so I think in that sense that ties into my second observation which is that our position is, in the administration, that we believe a strong Federal floor will actually reduce the incentives for States to want to legislate further in this area.

As an example, I might point out that in the HIPAA law itself that Congress passed 3 years ago, it is basically predicated on a notion of a very strong Federal floor, and to date at least I think States have not been desirous of or felt it was necessary to legislate beyond the HIPAA floor, and I think that is why we are placing so much emphasis on working with you and others to develop a Federal standard for confidentiality and protection that will reduce the need for additional State legislation.

Mr. CAMP. Thank you. Thank you, Mr. Chairman.

Chairman THOMAS. Well, to point out the absurdity of that statement, if I might, Minnesota currently has a provision which requires individual release for access to information. As a matter of fact, Mayo Clinic built its record on its epidemiological records which it now cannot do with any degree of confidence because it can only get 97 percent sign-off.

When you are doing research in key areas, obviously any hole in your data causes you problems. Let us take a Medicare patient from Minnesota. If Johns Hopkins wants to utilize that Medicare patient's medical records and tries to go through the State of Minnesota, obviously, they are going to have go through a sign-off procedure. I believe it is a three-denial effort or get the permission of the individual to do it. If Johns Hopkins goes to HCFA, can HCFA under the arrangement that we were discussing release the information of that Medicare patient who happens to live in Minnesota to Johns Hopkins?

Mr. HASH. The short answer is yes.

Chairman THOMAS. And John Hopkins being a reputable university and research structure would—of course you would be pleased to enter into an agreement with them?

Mr. HASH. We would review their proposal as we do all other research proposals to first see——.

Chairman THOMAS. Careful, Ben is here and so you would review it very quickly.

Mr. HASH. We would definitely review it in an expeditious manner and ascertain that the proposal, in fact, that the research questions being posed are ones that are important to our program, that the methodology that the proposal includes is one——.

Chairman THOMAS. As young people say, yada, yada, yada. The bottom line is, you will release that information to Johns Hopkins without the approval of the individual, and if Johns Hopkins tried to go through to get it from the State of Minnesota, they would have to follow a different procedure.

Mr. HASH. I have to disagree with one statement you made, Mr. Chairman, and that is, we would not release it without the permission of the individual. The individual in Medicare has already given their authorization for the use of these data to advance the program.

Chairman THOMAS. Let me see, I believe the trigger was you won't get Medicare benefits if you don't sign this sheet.

Mr. HASH. I don't believe so, Mr. Chairman. We have a variety of notices out there that when people sign up that indicates that there is a possibility that we would use personally identifiable data.

Chairman THOMAS. What is the turn-down ratio of Medicare benefits to people who refuse to receive Medicare benefits because they won't sign the release data?

Mr. HASH. I am not aware that there are refusals, Mr. Chairman.

Chairman THOMAS. Well, all right, we can go around all night on this if you want to. The answer you have given me, once you filter all of the procedure, is Minnesota will not release that information to Johns Hopkins unless the individual person signs off or it goes through a very elaborate three-denial check procedure.

Johns Hopkins can come and get it from HCFA without the patient's knowledge, and in fact, although I know Johns Hopkins wouldn't do it, based upon my earlier questions, Johns Hopkins could provide the information, if they were someone other than Johns Hopkins, to somebody else and unless it was done naked, high noon in the town square, by the way you detect transfer of information, cruising the net, you wouldn't know that it was transferred.

So all I am saying is it makes it very difficult for me to sit here and listen to you talk about building a floor and let the States go beyond the floor and have a structure that makes any sense at all because, as the sovereign, you are looking at the world, in my opinion, slightly differently than a private sector operation as reputable as Johns Hopkins in terms of its ability to get information.

I understand why you are not concerned, you are the sovereign, but this information is essential and I might say in fact more valuable in some of the private research activities in which the only way they are able to get the information is to hide behind you, the sovereign.

So when you talk about building a floor and letting States go beyond it, I think it gets kind of hypocritical when in fact that same entity can come to you and get the information they couldn't get

from a State. It doesn't make a whole lot more sense to build a uniform system that protects in a uniform way and that lets folks opt-out in areas where there is general agreement that it is necessary to allow under the police powers of the State protections for those purposes, but otherwise a uniform, structured, secure, confidential, preemption arrangement is the better way to go.

Gentleman from Maryland I know wants to inquire, and let me say before that, I am sorry he is no longer on the Subcommittee. I know he had to make a choice and under Democratic rules he became a powerful Ranking Member on another Subcommittee, and we don't have him here, but it is a pleasure to have him.

Mr. CARDIN. Well, thank you, Mr. Chairman, and let me thank you for your publicity on Johns Hopkins. I should point out it is my understanding that Johns Hopkins has a request before NIH for a research project related to dentistry. So I expect to get my friend from Wisconsin and my friend from California sponsoring that.

Let me, if I might, try to follow through on some of these questions.

In regards to individually identified medical records you are guided by the Privacy Act of 1974, I assume, and I have just tried to quickly read that statute and find that the language used there is significantly different than the language we are using here.

I don't see, for example, fraud and abuse or quality assurance or research or public health spelled out the same way that we generally have used those terms, but I assume you believe there is statutory authority within the Privacy Act of 1974 to release individually identified medical records for those particular purposes. And I guess my question to you is, we have been sort of dancing around this a bit, but if you were to be required to comply with State law and if the States had requirements for individual authorization for some of these uses, or a requirement that you individually notify the beneficiary of a request for information and an opportunity to opt-out without any further sanction to their Medicare benefits, is that workable for HCFA? Can you implement that? Is it costly to implement, and do you think that is good policy?

Mr. HASH. Well, with regard to the last set of questions, Mr. Cardin, we do have a procedure on research protocols that involves contacting individual beneficiaries that gives them the prior right to indicate that they do not want to participate in such research protocols.

Mr. CARDIN. How fast can you implement that? Is that a pretty fast procedure?

Mr. HASH. It is a pretty fast procedure. It usually involves a researcher who wants to draw a sample of our beneficiaries to contact them for some purpose that is outlined in their research proposal, and what we do is once we identify a sample, we actually write individual letters to them and give them this information about the opportunity to opt out if they do not wish to participate in it.

Mr. CARDIN. All right.

Chairman THOMAS. Will the gentleman yield briefly? Even Minnesota has a three follow-up kind of self-enacting operation. What

does HCFA have if you write the letter and there is no response to the answer?

Mr. HASH. We write the letter and then we require the researcher to wait a minimum of 10 days before contacting and then contact and reinquire as to whether the individual wants to participate or not, even though they have not replied to the letter they got from us.

Mr. CARDIN. If they don't reply, then that is assumed to be you can't release the information?

Mr. HASH. This is a case again of, Mr. Cardin, when an individual beneficiary is contacted by a researcher who wants to interview them.

Mr. CARDIN. If you don't get notification, they don't reply, can you use the records or not, if the beneficiary doesn't respond?

Mr. HASH. The researcher then may contact them and put the question again.

Mr. CARDIN. And there is still no response?

Mr. HASH. They contact them directly, you know, orally, by telephone or by visit.

Mr. CARDIN. So you need to get written authorization before you release under that circumstance?

Mr. HASH. I don't know that it requires a written release, but you have to get the authorization of the individual.

Mr. CARDIN. How do you know if you don't have it in writing?

Mr. HASH. I don't have an answer for that, Mr. Cardin, but I think—well, except I think in the research protocol we actually ask them to document the records about how they contacted the sample.

Mr. CARDIN. Mr. Hash, my time is running out. I really want to get an answer to this.

We don't know what the States could enact in this area. They could enact restrictions on your ability to use samples for fraud and abuse for all we know because of their protection on the individual's right of privacy, which is important. My question to you is, if the State of Maryland enacts a law that says you can't release information for fraud and abuse without specific authorization signed by the beneficiary, do you think that is a good policy to adhere to whatever the States indicate is the right policy on release of medical records?

Mr. HASH. I would hope that that kind of a policy would be built into the Federal floor that we are talking about, and therefore, if there were a conflict with Maryland law, that the Federal floor would obviously prevail there, but it is a question of designing the requirements in a sound way in the Federal floor to make sure we speak to those kinds of things.

Mr. CARDIN. We are in complete agreement there, and I expect there would be a cost associated, as I think you have already responded, to trying to comply with 50 different State standards as it relates to notice to the beneficiary and authorization and opt-outs or things like that. There has got to be a cost associated with that.

Mr. HASH. As I said, I think we need to address those issues in the context of what we require as a kind of uniform standard across all States.

Mr. CARDIN. And one last point, if I might, and that is that you said you were complying with the States to the extent possible. I was just handed the Maryland—someone compiled a book of all the different regulations—and in Maryland we have a requirement that insurers cannot disclose information except under a set of standards on release of information. Do you comply with the Maryland rules on disclosure of information currently?

Mr. HASH. I am not familiar with what the Maryland rules are, Mr. Cardin, but I would assume they follow the same kind of procedures that we follow under the Privacy Act, but I think——.

Mr. CARDIN. They are different. I am trying to match them up, and they are clearly different standards. There are some areas that are covered here that are not covered in the Privacy Act. Some in the Privacy Act are not covered here.

Mr. HASH. We follow the Privacy Act.

Mr. CARDIN. So you don't follow the Maryland general law on disclosure of medical information by insurers?

Mr. HASH. I just would like to reserve the right to review the Maryland law and see whether, in fact, we do or don't. But without saying that, I am certain that we don't.

Mr. CARDIN. Is there a conscientious effort to review the laws of the 50 States to try to comply with their privacy acts?

Mr. HASH. Not to my knowledge, Mr. Cardin, no. But when it is brought to our attention that someone asserts under a State law a particular right or privilege, obviously that would trigger our look at it and to see if there was a way that we could work with the State and the individual to work through that in a satisfactory manner. But as the Chairman points out, there is always a question of trying to balance the important rights of individuals to confidentiality and important rights of the State.

Mr. CARDIN. Well, I agree with your point and just appreciate your comment. We need to adopt adequate national standards in this area. I agree with the gentleman.

Chairman THOMAS. I thank the gentleman. Where is HCFA's headquarters?

Mr. HASH. In Baltimore, Maryland.

Chairman THOMAS. I thank the gentleman.

Gentlewoman from Connecticut wishes to do a follow up?

Mrs. JOHNSON of Connecticut. Thank you, Mr. Chairman.

I just wanted to go back to the issue of privacy. Under current practice at HCFA, do you routinely release individually identifiable health information to these contractors? I am talking about the payor contractor. I am talking about this 1,400 or so other people.

Mr. HASH. Researchers or other government agencies that have data use agreements with us, we do not routinely release individually identifiable data. It must go through the kinds of evaluation that I have outlined that are in our testimony before we do it. So we have a set of procedures to go through to determine when we will release.

Mrs. JOHNSON of Connecticut. When do you ever need to release individually identifiable data? I can see why you would need to release disease and symptoms and treatment data, but why would you have to have the person's name?

Mr. HASH. Well, for example, if we are engaged in an activity of collecting a third party liability, coordinating our benefits and trying to identify if the individual has another insurance policy that is liable——.

Mrs. JOHNSON of Connecticut. I consider that a payment problem.

Mr. HASH. OK. Within the context of research itself, there can be research projects—and I would defer to Dr. Hamburg here who is much more skilled in the research area than I am, but there can be research projects that advance our knowledge in terms of payment systems and how to do it more accurately or in terms of quality oversight that could require the use of personally identified information, but the presumption that we use at HCFA is that we start with the notion of trying to ascertain whether or not the research can be conducted successfully without personally identified information. That is where we start from, and only as a last resort do we agree to release personally identified information.

Ms. ARONOVITZ. I might be able to offer one example. It would be a longitudinal study, for instance, where you are looking at a particular person over time and looking at their health status over time. You might want to be able to identify that person and their records.

Mrs. JOHNSON of Connecticut. And that person has no right not to participate in that study? HCFA does not have to notify them that their data are going to be used on a longitudinal study?

Ms. ARONOVITZ. This is going to sound a bit bureaucratic, but in fact the person has been notified through the routine use conditions of disclosure that HCFA has in terms of guiding whether it can give out information to researchers.

Mrs. JOHNSON of Connecticut. I am interested that there are routine situations in which you would release somebody's personally identifiable information outside of HCFA. I mean, I understand for your payment system, but it seems to me that—and I don't know what percentage of these use agreements involve the release of individually identifiable information. Do you have any? Any of you have any comment on that? Whether it is most of them or—.

Mr. HASH. No. I think—as I say, I think our presumption is either to provide aggregated data whenever we can or at least encrypted data that is stripped of any individual——.

Mrs. JOHNSON of Connecticut. I appreciate that. The thing is, you know, how many of your agreements provide individually identifiable and how many provide encrypted data.

Mr. HASH. I would be happy to try to see if I can provide that for the record.

Mrs. JOHNSON of Connecticut. I think we need to know that, because I think in any bill we need to directly confront this issue, and I personally think the burden is on us to make the case that we wouldn't have to get permission.

[The following was subsequently received:]

As of July 21, 1999, there are 4,377 data use agreements in effect. Of these, 2,924 involve identifiable data and 1,453 involve encrypted data. The majority are with government agencies and researchers under contract to do work for the government; only 515 are not with Federal or State agencies or researchers under contract to such agencies.

Data Use Agreement (DUA) Statistics

DUAs Currently in Effect As of 7/21/99:	**4,377**
Total Currently In Effect Involving Identifiable Data:	**2 ,924**
Total Currently In Effect Involving Encrypted Data:	**1,453**
DUAs Initiated Within Last Year (1998-Current):	**1,911***
Total Identifiable:	**1,261**
Total Encrypted:	**650**
DUAs Initiated Within Last 5 Years (1994-Current):	**5,167***
Total Identifiable:	**3,950**
Total Encrypted:	**1,217**

***NOTE: Includes all DUAs initiated in the time period, both those currently in effect and those that have lapsed.**

DUAs In Effect Involving Identifiable Data by Category of Requestor

Category	*DUAs in Effect*
HCFA*	**563**
DHHS*	**864**
Other Government Agency*	**982**
Non-Government	**515**
TOTAL	**2,924**

***Including contract researchers**

Mr. HASH. Let me say if I may, Mrs. Johnson, that another thing that comes to mind in terms of where an individual identifier might be necessary in a research project, is when someone might be trying to answer questions related to how people were treated across different settings where there are different data systems with the claims information, and the only way to access that data across the different settings, whether it is in-patient, hospital or outpatient or home health or skilled nursing, is by being able to have the identifier that can link the claims for an individual so that you can actually see what happens to the patient from a hospital episode to an outpatient episode to a home health episode and answer some research questions associated with appropriate types of care.

So that is an example of where, in order to access the data on services that an individual has actually received, you can't get it unless you have an identifier number that links that data to a specific individual.

Mrs. JOHNSON of Connecticut [presiding]. I think it is very concerning that people would not know when these data were going to be used, that, you know, agreements that you have literally no control over, you just really can't control the number of agreements you are going to have, and really this gives no privacy protection for Medicare participants when your agency has allowed access by a researcher to their files.

So I think that we are not going to solve this here, but I think as we move through this bill—I mean, when I look at the battle that went on in H.R. 10 around privacy issues, health issues information is just so much more important to people individually that I think we are going to have to deal with this up front and clean, and we can't sort of mask it behind HCFA's judgment. At a certain point, if your information is going to be released with your name identified to it——.

So, anyway, we need to move on to the next panel, but you get the gist of my concerns.

Mr. KLECZKA. I was waiting for the second round.

Mrs. JOHNSON of Connecticut. Briefly. They want us to move on to the next panel because some of them have to leave.

Mr. KLECZKA. I agree with the gentlelady that where to draw that line is going to be very difficult for this Subcommittee and for this Congress. Ms. Hamburg, in your testimony you talked about the public responsibility. I agree with you that an individual's privacy and medical privacy can never be absolute. From the dialog that we have been listening to, some people are stating there is an absolute right for all these other entities and I am saying that is clearly wrong. I would rather err on the side of personal privacy than going that way.

The gentlelady just referenced the bill we had before the House the other day on banking modernization, H.R. 10. I am sure you are aware of the controversy as it pertains to medical records in that bill. Do you want to comment on that and also briefly com-

ment on this whole question of preemption? I am getting very confused here.

First of all, we are told by the majority party that we have to defer to State rights because that is where all the knowledge and the power is. As a former legislator in the State of Wisconsin, I totally disagree with that. But, nevertheless, if they say so, maybe it is true.

The Senate debated the Patients' Bill of Rights and, they argued that the States have to be recognized in their ultimate power over the rights of patients in medical care, and so the Senate only addressed the ERISA plans that cut down by almost two-thirds the number of people covered by that bill.

Now on the other side of the Capitol, when it comes to medical privacy, the arguments is be damned with States' rights because we are the all-powerful and knowing.

And so I am saying, Mrs. Johnson, to you and your Republican colleagues, make up your mind so I can get on the same script with you. I want to be helpful, but if States should have rights, let us do so. If States shouldn't have rights, I might buy into that program, but we can't have it both ways depending on the issue. The inconsistencies are abundant.

Dr. Hamburg, would you want to respond—not to that last point, but to the previous point on the modernization bill?

Dr. HAMBURG. On H.R. 10?

Mr. KLECZKA. H.R. 10 and the preemption issue. Those are two big issues here.

Dr. HAMBURG. Starting with the preemption issue, I think obviously, as the discussion today has indicated and many other discussions in recent months, it is a very complicated issue. And as a relative newcomer to Washington and somewhat naive, I have to say that I was originally confused about where people were lining up on this issue. But I think that what we do all agree on is that there is a need for a strong and comprehensive set of national protections for privacy of health care information and that we need to be very thoughtful about what those are. We need to reflect many of the kinds of concerns discussed today, but we need a strong and comprehensive set of national standards.

We think that, given how rapidly medical issues and technology are changing, how different certain States are in terms of the demographics and patterns of disease, and given that different States are in different places in terms of confidentiality and privacy protection laws at the present time, we don't want to put a straitjacket on States so that they can't be innovators and so that they cannot adapt to the unique needs of their States and their citizens, but I think we all absolutely agree on the need for a comprehensive set of national standards that have both breadth and depth to address the kind of concerns we are talking about today.

With respect to H.R. 10, we think that the issue of medical privacy is sufficiently important and complicated that it should really be dealt with in a piece of legislation that is targeted to the issue of medical privacy and that it is a mistake to try to address it in a piecemeal fashion or as a rider to another bill. We would really be best served not to try to tinker with that, but instead to strike it all together and focus on this important set of issues through a

piece of legislation that targets directly the issues we are discussing today.

Mr. KLECZKA. Thank you very much.

Mrs. JOHNSON of Connecticut. I thank the panel for your testimony and we appreciate you being here this afternoon and let me call the next panel.

Paul Clayton, Richard Smith, Janlori Goldman and Thomas Jenkins. The Chairman will be returning as soon as possible, but we will proceed.

Good afternoon. We will start with Paul Clayton, Ph.D., Senior Informaticist, Intermountain Health Care, Salt Lake City, on behalf of the American Hospital Association. Please proceed, Dr. Clayton.

STATEMENT OF PAUL D. CLAYTON, PH.D., SENIOR INFORMATICIST, INTERMOUNTAIN HEALTH CARE, SALT LAKE CITY, UTAH, ON BEHALF OF THE AMERICAN HOSPITAL ASSOCIATION

Mr. CLAYTON. I am Paul Clayton of Intermountain Health Care, and I am also President of the American Medical Informatics Association, a member of the health privacy working group whose report was released last week, and I chaired the National Research Council's 1997 study "For The Record: Protecting Electronic Health Information."

I am here today on behalf of the American Hospital Association, its 5,000 hospitals, health systems and other providers. The AHA supports strong Federal legislation establishing uniform national standards for all who use protected health information, with strong penalties for inappropriate use. Our comments today focus on how hospitals use and protect patient information. Our longstanding confidentiality principles cover a broader range of critical patient privacy issues, and I have attached them to my written statement.

People who make these decisions affecting the health of patients must know about the medical and family history, allergies to drugs, previous diagnostic results, current medications, previous surgeries or therapies and chronic problems. Access to this information dramatically affects the level of care that can be provided.

For the past 14 years, IHC has used clinical data systems to substantially improve patient care. Here are four examples.

First, for inpatient prescriptions, a computerized order entry system warns physicians of potential allergies and drug-to-drug interactions and calculates the ideal dose levels. That dose system has reduced adverse drug reactions by two-thirds.

Second, improved management of mechanical respirators for patients with acute respiratory distress syndrome. In these most seriously ill patients, mortality rates fell from 90 to 60 percent.

Third, improved management of outpatient diabetic patients. The proportion of patients brought to normal blood sugar levels improved from less than 30 percent to more than 70 percent.

And, fourth, accountability for our performance. IHC assembles and reports medical outcomes, patient satisfactions and cost outcomes for major clinical processes.

These examples are all successful because patient identifiable information flowed smoothly among the providers that needed it.

Two provisions in various proposals could stem that appropriate flow of information. The first is an opt-out where patients could pick and choose which health information providers could see. This mosaic of access restrictions could greatly hinder our ability to render care. For example, when a patient seeks care within our system, IHC laboratory analyzers feed the patient's blood tests directly into our computers. This improves our ability to make accurate results immediately available, but it also necessarily eliminates our ability to process laboratory tests without using the electronic medical record.

Second, while we strongly support the development of policy to restrict access privileges, we are concerned that some proposals would require providers to limit the scope of disclosures to the minimum, however that is defined, amount necessary for the specific purpose at hand. This means providers must repeatedly predict the exact present and future implications for every piece of information. The intellectual effort needed to ensure each person's compliance becomes overwhelming.

I have reviewed how we use patient information to improve care, and now I would like to review how we protect the information. Every employee, health care professional, researcher or volunteer must sign an agreement that they will only look at or share information for specific legitimate purposes of performing their health care delivery assignment. Each new employee undergoes training in IHC confidentiality policies which are set forth in a manual of more than 60 pages. We impose consequences, including termination, for improper use or handling of confidential information. We use audit trails to monitor and access the electronic patient records. In the electronic format, we are able to separate patient identifiers from the rest of the clinical record, and we require formal review, approval and oversight of research that uses patient data.

Let me conclude by saying that the technology to protect patient information is available, but without a Federal mandate there is little incentive to make such an investment. We urge Congress to enact legislation that will help hospitals, physicians, nurses and others coordinate care and improve quality and, at the same time, protect our patients' medical information from misuse.

Thank you.

[The prepared statement and attachment follow:]

Statement of Paul D. Clayton, Ph.D., Senior Informaticist, Intermountain Health Care, Salt Lake City, Utah, on behalf of the American Hospital Association

Mr. Chairman, I am Paul D. Clayton, PhD, senior informaticist at Intermountain Health Care (IHC) in Salt Lake City, UT. IHC is an integrated health care delivery system that operates in Utah, Idaho and Wyoming. The IHC system includes 23 hospitals, 78 clinics and physician offices, 23 outpatient primary care centers, 16 home health agencies, and 400 employed physicians. In addition, our system operates a large Health Plans Division with enrollment of 475,000 directly insured, plus 430,000 who use our networks through other insurers.

I am testifying today on behalf of the American Hospital Association (AHA), which represents nearly 5,000 hospitals, health systems, networks, and other providers of care. We appreciate this opportunity to present our views on an issue important to hospitals, health systems, and the patients they serve: the confidentiality of protected health information.

PROTECTING PATIENTS' TRUST

Every day, thousands of Americans walk through the doors of America's hospitals. Each and every one of them provides caregivers information of the most intimate nature. They provide this information under the assumption that it will remain confidential. It is critical that this trust be maintained. Otherwise, patients may be less forthcoming with information about their conditions and needs-information that is essential for physicians and other caregivers to know in order to keep people well, ease pain, and treat and cure illness.

If caregivers are not able to obtain and share patients' medical histories, test results, physician observations, and other important information, patients will not receive the most appropriate, high-quality care possible.

Our members consider themselves guardians of this information. That is why AHA has long supported the passage of strong federal legislation to establish uniform national standards for all who use patients' personal medical information-what we refer to as protected health information. We have been asked to focus our comments today on how hospitals use and protect patient information to enhance the quality of the patient care they deliver. Our longstanding principles for the confidentiality of health information cover a broader range of critical patient privacy issues, and we have attached them for your information. We will measure any federal privacy legislation against these principles in their entirety.

Confidentiality of health information is an issue that affects all of us personally. We live in a time of rapidly advancing technological improvement, when the world seems to get smaller as computers get more powerful and databases get bigger. This technological change can be positive—it has led to significant improvements for both health care providers and their patients—but it worries people who are justifiably concerned about how information about them will be used.

In health care, we must take the steps necessary to protect that information from those who would misuse it. We need strong, uniform federal legislation to do it.

First and foremost, because we as hospitals and health systems put our patients first, we must restore and maintain people's trust in the privacy and confidentiality of their personal health information. Federal legislation can do this by establishing a uniform national standard for the protection of this information—including genetic information—a standard that balances patient privacy with the need for information to flow freely among health care providers.

PRIVACY AND HEALTH CARE OPERATIONS

Health care is increasingly provided by groups and systems of providers, as opposed to individual providers. These new systems create opportunities for real improvements, but they rely heavily on a free flow of information among providers. Patient confidentiality is of the utmost importance. But in order to ensure that care can be coordinated and the patient's experience is as seamless as possible, information must be accessible to all providers who treat the patient.

There is very little disagreement that access to information is important in the delivery of care to patients, and in the system of payment for that care. Controversy has developed, however, over the definition of "health care operations"—those essential functions performed by providers to ensure that they maintain and improve the quality of the care they deliver, train current and future caregivers, and adhere to the laws and regulations that govern these daily activities. AHA believes that protected health information must be available to providers so that these functions can be performed efficiently and effectively.

INFORMATION BREEDS HEALTH CARE SUCCESS STORIES

At IHC, we believe, as does the AHA, that individuals who are making decisions that affect the health of another person must know about past medical and family history, allergies to drugs, previous diagnostic results, current medications, previous surgeries or therapies, and chronic and acute problems. Because the primary caregiver is not present all the time, because others are asked for consultive opinions, and because humans have limited memory, access to medical record information dramatically affects the level of care that can be provided. In some cases, the absence of information increases the cost of diagnosis and treatment by causing tests to be repeated because the results of an earlier tests are not available.

Among the benefits of improved access are an enhanced ability to generate bills and collect payment, and to transmit information to payers and analyze the costs of providing care. Care is also improved when a caregiver has access to the medical record. A physician or other health care worker who knows what drugs a patient is taking, a list of previous problems, a history of family predisposition to certain

illnesses, and current laboratory results, will make better decisions about how to diagnose and treat a patient.

At IHC, we have, for the past 14 years, used clinical data systems to substantially improve patient care in a wide range of circumstances. Here are a few examples.

• *Improved timing of delivery of pre-operative antibiotics to prevent serious post-operative wound infections*. Our wound infection rate fell from 1.8 percent to 0.4 percent, representing, at just one of our 23 hospitals, more than 50 patients per year who now do not suffer serious, potentially life-threatening infections. We also saved the cost of treating those infections, which, at that hospital, was estimated at $750,000.

• *Improved support for inpatient prescriptions*. A computerized order entry system warns physicians, at the time they place the order, of potential allergies and drug-to-drug interactions. It also calculates ideal dose levels, using the patient's age, weight, gender, and estimates of patient-specific drug-absorption and excretion rates, based on laboratory values. That system has reduced allergic reactions and overdoses by more than two-thirds.

• *Improved management of mechanical respirators for patients with acute respiratory distress syndrome*. In the most seriously ill category of these patients, mortality rates fell from more than 90 percent to less than 60 percent.

• *Improved management of diabetic patients in an outpatient setting*. The proportion of patients brought to normal blood sugar levels improved from less than 30 percent to more than 70 percent. Major studies of diabetes demonstrate that this kind of shift in blood sugar translates to significantly less blindness, kidney failure, amputation and death. Others indicate it should reduce the cost of treatment for diabetes patients by about $1,000 per patient per year.

• *Improved treatment of community-acquired pneumonia*. By helping physicians more appropriately identify patients who needed hospitalization, choose appropriate initial antibiotics, and start antibiotic therapy quickly, we were able to reduce inpatient mortality rates by 26 percent. That translates into about 20 lives saved at 10 small rural IHC hospitals when we first worked on this aspect of care. It also reduced costs by more than 12 percent.

• *Accountability for health care delivery performance*. IHC has begun to assemble and report medical outcomes, patient satisfaction outcomes, and cost outcomes for major clinical care processes that make up more than 90 percent of our total care delivery activities. We aggregate and report those data at the level of individual physicians; practice groups; hospitals; regions; and for our entire system. We use the results to hold each health care professional and our system accountable for the care we deliver to our patients, and to set and achieve care improvement goals. We believe that this system will eventually allow IHC to accurately report our performance at community, state and national levels, and help individuals and groups make better health care choices.

All of the examples above were successful because patient information—not just individual patient information, but also information about populations of patients—was available, and flowed smoothly among the providers that needed it.

Potential Disruptions to the Free Flow of Information

There are two provisions in various patient privacy proposals that could have the unintended effect of placing enormous barriers in front of providers' ability to appropriately use information for these and similar purposes.

The first is what has been referred to as the "opt out," where patients would have the ability to prevent providers from sharing the patient's information regardless of how important such a disclosure might be.

The problem with such an opt out is that it sacrifices hospitals' ability to deliver high-quality care to the individual involved, as well as to other patients. For example, IHC's laboratory analyzers feed directly into our computer system. When we committed to that link, we not only significantly improved our ability to deliver excellent care to all of our patients, but also necessarily lost our ability to process blood laboratory tests without using the electronic medical record.

In addition, a patient who might decide to prevent his or her records from being shared among providers is, effectively, reducing the quality of health care he or she may receive in the future. This is because, without access to that patient's records, providers simply cannot make well-informed decisions. At the same time, removing the patient's treatment information as a factor in overall health care statistics degrades the overall integrity of the health care information flow. In other words, if less is known, less can be learned, and the overall quality of care could be affected.

The second potential problem we see being discussed is a requirement, included in several patient privacy proposals, that providers must limit the scope of medical

information disclosures to no more than what is necessary for the specific purpose of the disclosure. Penalties would be levied, according to the proposals, presumably if too much information were to be provided.

Health care providers, who deal with a mountain of information every day, simply cannot be expected to determine the exact need for every piece of information and the exact measurement of information that may be required to meet that need. The threat of penalties makes the proposals worse, and is sure to inhibit the free flow of important information. In addition, proper safeguards should already be in place that would prevent the misuse of patient information, so that requiring providers to justify each disclosure would be unnecessary.

Proper policies and procedures will ensure that patient information is used only where it is needed to benefit the health care services provided to an individual patient, or to improve the overall health care system through statistics and analysis.

SAFEGUARDING PATIENT INFORMATION

IHC and the AHA support strong, uniform federal confidentiality standards that buttress our health care delivery and clinical research work. IHC has placed appropriate protection of patient confidentiality and privacy at the forefront of our institutional values. Those values complement a parallel mission to provide the best possible health maintenance and disease treatment to those who trust their care to our hands. Achieving this requires the use of population-level patient data as well as individual patient data.

IHC uses enforceable corporate policy to maintain confidentiality not just for patients, but for health care professionals and employees as well, in those areas that are clearly health care delivery operations (such as direct patient care delivery; billing for services; quality review of individual patient records, including mortality and morbidity conferences; resource planning; unit performance evaluation; quality improvement and disease management; and retrospective epidemiologic evaluations of program performance). The core of these policies and enforcement activities include:

• We require every employee, health care professional, researcher or volunteer to sign a confidentiality agreement stating that they will only look at or share information for the specific purpose of performing their health care delivery assignment on behalf of our patients. We require each new employee to undergo training in IHC confidentiality policies, which are set forth in a manual that numbers more than 60 pages and represents more than five years of discussion and cross-testing.

• We impose consequences—including termination—for improper use or handling of confidential information.

• To the extent that we have implemented an electronic medical record, we are able to monitor access to patient records (an ability not available for paper records). We use that system as one important method of monitoring and enforcing our confidentiality policy. We utilize software controls, including warnings on log-on screens, unique log-on passwords, and computerized audit trails. In the near future, we hope to bring on-line the ability of all patients to review a list of every individual who has accessed their electronic medical record for any purpose.

• We segregate our electronic databases, separating patient identifiers from the remainder of the clinical record. Outside of direct patient care and individual record review for quality assurance, most health care delivery operations do not require access to identifiable data. IHC's data access policies regulate access to patient information using strict "need to know" criteria by job description. While we afford tight access control to all of our information, the identifiable portion of the record receives the highest level of protection.

• We are studying ways to segregate the core clinical record itself, so that particularly sensitive information—for example, HIV status, reproductive history, or mental health status—are only available on a strict "need to know" basis, even to the front-line care delivery team.

In addition, we require full institutional review board (IRB) review, approval and on-going oversight for any research project that involves experimental therapy, patient randomization among treatment options, or patient contact for research purposes. Indeed, the IHC system has 12 IRBs, but we do not look to them as our sole—or even our primary—means to protect confidentiality. Most of the risks to patient confidentiality come in day-to-day care, as physicians and nurses routinely access identifiable patient medical records, both paper and electronic, to deliver care. Instead, we rely upon the extensive array of enforceable policies and procedures listed above.

If IRB review of each of these health care operations were required, many—if not most—of the operational care delivery and health outcome improvements described earlier could not function on a day-to-day basis. The volume of review would be

staggering, far beyond the capacity of any reasonable system of individual review and follow-up oversight.

CONCLUSION

As an integrated health care delivery system, IHC is responsible for the health outcomes of the patients who seek care from our system. In order to treat our patients and improve the health outcomes of the entire population we serve, we must be able to share information among IHC entities—our physicians, our hospitals, and our health plans. IHC has developed state-of-the-art electronic medical records and common databases to facilitate this communication, to make sure our physicians have complete information when treating patients . We have put in place an extensive array of enforceable confidentiality protections that are constantly updated and improved.

We urge this panel to ensure that confidentiality legislation does not unintentionally prevent the creation of these common internal, operational databases, or limit the types of data that can be shared within an integrated delivery system. Such action would severely limit a health system's ability to measure and improve the health care it delivers.

The outstanding care that physicians, nurses and others deliver at IHC and in hospitals and health systems across America relies more and more on coordination of care and on effective quality improvement. Individually identifiable health information is integral to such operations, and the free flow of this information—properly safeguarded from misuse—is critical to our ability to continue providing high-quality health care for patients and communities.

American Hospital Association

Principles for Confidentiality of Health Information

Every day, thousands of Americans walk through the doors of America's hospitals. Each and every one of them provides caregivers information of the most intimate nature. They provide this information under the assumption that it will remain confidential. It is critical that this trust be maintained. Otherwise, patients may be less than forthcoming with information about their conditions and needs—information that is essential for physicians and other caregivers to know in order to keep people well, ease pain, and treat and cure illness.

If caregivers were not able to obtain and share patients' medical histories, test results, physician observations, and other important information, patients would not receive the most appropriate, high-quality care possible. Our members consider themselves guardians of this information, which is why AHA has long supported the passage of strong federal legislation to establish uniform national standards for all who use health information.

In health care, we must take the steps necessary to protect patients' confidential information from those who would misuse it. We need strong, uniform federal legislation to do it.

AHA goals for legislation

First and foremost, because we as hospitals and health systems put our patients first, we must restore people's trust in the privacy and confidentiality of their personal health information. Federal legislation can do this by establishing a uniform national standard for the protection of health information—including genetic information—a standard that balances patient privacy with the need for information to flow freely among health care providers. The AHA believes that federal confidentiality legislation must meet the following goals:

• Allow patients and enrollees access to their medical information, including the opportunity, if practical, to inspect, copy, and, where appropriate, add to the medical record. Patients have a right to know what information is in their records. This level of accountability encourages accuracy and has the added benefit of encouraging patient involvement in their care.

• Preempt state laws that relate to health care confidentiality and privacy rights, with the exception of some public health laws. Health care today is delivered through providers that are linked together across delivery settings, and in organizations that cross state boundaries. AHA believes that the best way to set important standards for confidentiality of health information is to do so uniformly—through a *strong federal law*. This law must be both a floor *and* a ceiling, preempting all state laws with which it may conflict, weaker or stronger. Only through such a uniform law can patients' confidential information be equally protected regardless of the state in which they live or travel.

• Be broad in its application, covering all who generate, store, transmit or use individually identifiable health information, including but not limited to providers, payers, vendors, and employers. Patient confidentiality cannot be ensured unless standards are applied to *all* who may have access to their health information. Legislation should cover all types of individually identifiable health information, including sensitive issues such as substance abuse, mental health, and genetic information.

• Strike an appropriate balance between patient confidentiality and the need to share clinical information among the many physicians, hospitals and other caregivers involved in patient care. Care is increasingly provided by groups and systems of providers as opposed to individual providers. These new systems create opportunities for real improvements, but they rely heavily on a free flow of information among providers. Patient confidentiality is of the utmost importance. But in order to ensure that care can be coordinated and the patient's experience is as seamless as possible, information must be accessible to all providers who treat the patient.

• Recognize that a hierarchy of need exists among users of health information. Access to individually identifiable information is essential for patient care. Such access may also be necessary for provider and health care system efforts to measure and improve the quality of care. All internal and external uses of patient information must be evaluated as to whether the use of individually identifiable information is justified.

• To limit its potential misuse, all within the health system should restrict the availability of individually identifiable information. Technology is available to do this, through encryption, audit trails, and password protection, for example. Another method for restricting the availability of individually identifiable information is to aggregate information whenever possible. Patients should be assured that unique, identifiable information about them is available for their treatment, but that its availability for other uses is tightly controlled.

• Include sufficient civil and criminal penalties to deter inappropriate disclosure of individually identifiable information. The level of such sanctions should vary according to, the severity of the violation. At the same time, any penalty imposed must take into account good-faith efforts by providers who establish data safeguards, educate employees about complying with these safeguards, and attempt to maintain secure recordkeeping systems.

Mrs. JOHNSON of Connecticut. Thank you very much, Dr. Clayton.

Dr. Richard Smith, Professor of Psychiatry at the Centers for Mental Health Services Research, University of Arkansas on behalf of the American Medical Colleges.

Dr. Smith.

STATEMENT OF G. RICHARD SMITH, JR., M.D., PROFESSOR OF PSYCHIATRY AND MEDICINE, UNIVERSITY OF ARKANSAS FOR MEDICAL SCIENCES, ON BEHALF OF THE ASSOCIATION OF AMERICAN MEDICAL COLLEGES

Dr. SMITH. Thank you, Mrs. Johnson and Members of the Subcommittee. I am Dr. G. Richard Smith from the University of Arkansas for Medical Sciences, a practicing psychiatrist and director of one of the Nation's largest mental health services research groups as well as our college of medicine's health services research program. I am speaking today on behalf of the Association of American Medical Colleges, the AAMC.

AAMC strongly supports the general intent of current congressional efforts to strengthen the protection of individual's personally identified health information from inappropriate and harmful misuse that can lead to discrimination or stigmatization. In the interest of public health, this protection should take into account the need for health services and biomedical researchers to have ready

access to archival materials on relevant populations required to generate meaningful conclusions regarding the incidents and expression of diseases in specified populations, the beneficial and adverse outcomes of particular therapies and the medical effectiveness and economic efficiency of the health care system.

In attempting to deal with the difficult issues of medical information confidentiality, legislative efforts should be directed toward requiring the establishment of strong administrative, technical and fiscal safeguards to protect the confidentiality, security, accuracy and integrity of information that directly identifies an individual. Legislation should also specify stiff criminal, civil and administrative penalties for intentional or recklessly negligent actions that violate medical information confidentiality. With such stringent security requirements in place, AAMC believes legislation should refrain from attempting to construct elaborate barriers to the relatively unimpeded flow of medical information that is required for the promotion of a comprehensive national agenda medical research.

In particular, the AAMC is concerned about secondary research which utilizes patients records as research material and does not involve interaction with individual patients. For example, mental health services research on patient records has established that pediatric patients treated for attention deficit disorder, or ADHD, were far less likely to use and become dependent upon illegal drugs during young adulthood than people with ADHD who did not receive appropriate information.

Archival data was also critical to establishing the postmarketing safety and effectiveness of drugs. Since many patients with major mental illness require long-term medication treatment, the effects of chronic use of new drugs cannot be adequately assessed in conventional premarketing clinical trials. The consequences can only be recognized by retrospective study of large populations over prolonged periods of time. Archival data were essential in establishing the safety of a new generation of antidepressant drugs on the fetuses of mothers who had been receiving these drugs chronically for the treatment of depression.

In sum, access to archival data is critical to assuring the health of patients with mental illness, just as with any other medical illness. Archival data also help us to identify the relative contribution of genetic, environmental and developmental factors related to the risk of specific mental disorders in families across generations.

The uncertainty and predictability of secondary research make the applicability and traditional informed consent procedures problematic. For secondary research using medical information that is individually identified, the AAMC believes a statutory requirement of specific authorization would be unwise and could seriously bias and therefore undermine the integrity of vital research databases. Rather, the Association recommends that all such proposed research should be reviewed by an institutional review board or equivalent mechanism to ensure that research is credible, the need for individually identifiable medical information is legitimate and the investigators have in place confidentiality policies and procedures required by statutes.

Patients' confidence in the medical research use of their personal medical information would be greatly enhanced by the inclusion of a statutory assurance of confidentiality as provided in S. 881, sponsored by Senator Bennett, and H.R. 2470, sponsored by Representative Greenwood. Such an assurance would prohibit any unauthorized attempts to gain access for nonresearch purposes to individually identified health information contained in research databases.

The AAMC strongly supports the position of new Federal information privacy legislation preempting State privacy laws. There is a compelling Federal interest in ensuring that medical research is facilitated and not hindered by this disorganized patchwork of State privacy laws. The AAMC commends this Subcommittee for convening this hearing to address the need for confidentiality legislation and the efforts of Chairman Thomas and Representative Cardin in crafting legislation that would enhance security of medical records.

This concludes my statement, and I would be happy to answer any questions the Committee has.

[The prepared statement follows:]

Statement of G. Richard Smith, Jr., M.D., Professor of Psychiatry and Medicine, University of Arkansas for Medical Sciences, on behalf of the Association of American Medical Colleges

Mr. Chairman and members of the Subcommittee, I am Richard Smith, M.D., Professor of Psychiatry and Medicine at the University of Arkansas for Medical Sciences. I am a practicing psychiatrist and also conduct mental health services research. I lead the Centers for Mental Health Services Research at the University of Arkansas, which is one of the nation's largest mental health and services research groups, as well as our College of Medicine's health services research program. I am a recent past member of the National Mental Health Advisory Council for the National Institute of Mental Health (NIMH). I also chaired the NIMH Initial Review Group for mental health services research, which reviews virtually all of the mental health services research grant applications submitted to NIMH.

I am speaking today on behalf of the Association of American Medical Colleges (AAMC). The AAMC represents the nation's 125 accredited medical schools, nearly 400 major teaching hospitals and health care systems, more than 87,000 faculty in 89 professional and scientific societies, and the nation's 67,000 medical students and 102,000 residents.

The AAMC strongly supports the general intent of current Congressional efforts to strengthen the protection of individuals' personally identified health information from inappropriate and harmful misuse that can lead to discrimination or stigmatization.

Confidentiality legislation must acknowledge the compelling public interest in continuing to ensure access to patient records and other archival materials required to pursue biomedical, behavioral, epidemiological and health services research. Medicine has always been, and largely remains to this day, an empirical discipline, and the history of medical progress has been created over many centuries from the careful, systematic study of normal and diseased individuals. From those studies has emerged our present level of understanding of the definition, patterns of expression and natural history of human diseases, and their responses to ever improving strategies of diagnosis, treatment, and prevention. In particular, health services researchers continue to depend upon the ready accessibility of archival materials to collect the large and appropriately structured and unbiased population samples required to generate meaningful conclusions regarding the incidence and expression of diseases in specified populations, the beneficial and adverse outcomes of particular therapies, and the medical effectiveness and economic efficiency of the health care system. Indeed, in the present climate of major public concern about the costs, quality, and efficiency of our rapidly changing health care delivery system, the need to support and promote such retrospective epidemiological and health services research has become an urgent priority.

The AAMC strongly believes that in attempting to deal with the difficult issues of medical information confidentiality, the most feasible and effective approach is

not to erect costly and burdensome new barriers to accessing medical information required to conduct research. Rather, legislative efforts should be directed, as most of the current proposals attempt to do, toward requiring the establishment of strong administrative, technical and physical safeguards to protect the confidentiality, security, accuracy and integrity of information that directly identifies an individual. Included among these safeguards should be strong institutional policies of confidentiality, which might appropriately meet federal standards to be developed. To complete the "security package," legislation should specify stiff criminal, civil, and administrative penalties for intentional or recklessly negligent actions that violate medical information confidentiality. With stringent security requirements of this kind in place, the AAMC believes that legislation should refrain from attempting to construct elaborate barriers to the relatively unimpeded flow of medical information that is required for the promotion of a comprehensive national agenda of medical research.

Given the substantial penalties contained in the confidentiality bills now in draft or under consideration, it is imperative that bills' definitions be crafted with great clarity. Of particular importance is the definition of "individually identifiable health information," the class of medical information most in need of protection from inappropriate disclosure and harmful misuse, and correspondingly of "non-individually identifiable health information," the class that would fall outside the purview of confidentiality legislation. The AAMC believes that the protected class of medical information should be sharply circumscribed and limited to "information that directly reveals the identity or provides a direct means of identifying an individual." Such a definition is least ambiguous and incorporates the sum and substance of the information that the public is most concerned to protect.

Correspondingly, the definition of "nonidentifiable health information" should encompass "information that does not directly reveal the identity of an individual." This definition should explicitly include coded or encrypted information (sometimes called "anonymized"), whether or not the information is linkable to individuals, as long as the encryption keys are secured and kept separate from the encrypted information itself. The justification for including encrypted, linkable information in the definition of nonidentifiable health information is significantly strengthened by adding additional provisions that make it a crime to attempt to use encrypted patient data to discover an individual's identity by any means other than the lawful use of an encryption key.

The AAMC believes that a set of properly constructed definitions of protected health information and nonidentifiable health information will serve both to foster medical research and establish an incentive system for using nonidentifiable health information in such research to the maximum extent practical.

The AAMC is especially concerned about the conduct of secondary research on archival patient materials. These studies utilize patient records as primary research materials and do not involve interaction with individual patients. In mental health services research, for example, secondary research on patient records has established that pediatric patients treated for attention deficit disorder (ADHD) were far less likely to use and become dependent upon illegal drugs during adolescence and young adulthood than patients with ADHD who had not received appropriate treatment. Archival data were essential in recently establishing the safety of the new generation of antidepressant drugs (selective serotonin reuptake inhibitors) on the fetuses of mothers who had been receiving these drugs chronically for the treatment of depression. As these examples suggest, archival patient data are critical to establishing the post-marketing safety and effectiveness of drugs. Since many patients with major mental illness require long-term medication treatment, and the effects of chronic use of new drugs cannot be adequately assessed in conventional pre-marketing clinical trials, the consequences can only be recognized by retrospective study of large populations over prolonged periods of time. In sum, access to archival data is critical to assuring the health of patients with mental illnesses.

Archival data can also be useful in identifying risk factors related to the onset of a mental illness. For example, there continues to be strong interest in the role of genetic factors in the etiology of major mental illnesses such as schizophrenia, bipolar disorder, major depression and obsessive compulsive disorder. In seeking clues that could help to direct future research in this area, it is critical for researchers to be able to access archival patient care records, for example, of deceased family members of patients involved in genetic studies. It is possible that mental illnesses that are now not linked in any way might be found to cluster in families in a manner that suggests a common genetic etiology. Archival data can also help to clarify the relative contribution of genetic, environmental and developmental factors related to risk of specific mental disorders in families across generations.

In contrast to the typical interventional clinical research study, in which researchers directly interact with patients in well-defined protocols and can provide them with the detailed information required for informed consent, the uncertainties and unpredictability of secondary research make the applicability of traditional informed consent procedures problematic. Accordingly, under the provisions of the federal Common Rule, such retrospective research has been singled out for special attention and, under the criterion that the proposed research is commonly deemed to be of no more than minimal risk to research subjects, has typically been handled by Institutional Review Boards (IRBs) by use of the expedited review mechanism, or even on occasion, by wavier of review.

For secondary research using medical information that is individually identified, i.e. that fall within the definition of protected health information, the AAMC believes that a statutory requirement of specific authorization would be unwise and could seriously bias, and thereby undermine the integrity of these vital research databases. Rather, the Association recommends that all such proposed research must be reviewed by an IRB or equivalent mechanism. The reviewing body should be required to determine that (1) the organizational setting in which the research will be conducted is in conformity with statutory requirements for safeguarding medical information confidentiality; (2) the research requires the use of individually identifiable patient information and could not be performed without it; and (3) it would not be practicable or feasible for the investigators to attempt to obtain individual informed consent from the subject population. Such a review procedure would sufficiently protect the privacy interests of the research subjects, while at the same time continuing to facilitate the conduct of a broad spectrum of beneficial secondary research on archival patient materials. Instead of mandating specific consent for secondary research, the Association recommends that IRBs or other equivalent review bodies should continue to review such research and determine whether specific consent is necessary on a project by project basis.

In addition, AAMC firmly believes that patients' confidence in medical research uses of their personal medical information would be greatly enhanced by the inclusion of a "statutory assurance of confidentiality" as provided by S. 881 sponsored by Senator Bennett and H.R. 2470 sponsored by Rep. Greenwood. Such an assurance would prohibit any unauthorized attempts to gain access for non-research purposes to individually identifiable health information contained in research databases, including Federal, State, or local civil, criminal, administrative, legislative, or other proceedings. Consequently, researchers could confidently assure patients that all individually identifiable medical information that might be used in the course of research would be shielded from forced disclosure to anyone, including family members, employers, insurers, health care organizations or legal or judiciary processes.

The "statutory assurance of confidentiality" provision is modeled on the existing Certificate of Confidentiality issued by the National Institutes of Health on a project by project basis. The origin of the Certificate of Confidentiality dates back to the Vietnam War era. Scientists and policy makers were very concerned about the extent of heroin use by our soldiers in Vietnam—and the danger that they might be permanently addicted when they returned to the United States. Since heroin possession was then—and is—a crime, it would have been impossible to enlist the subjects necessary to conduct a follow-up study of heroin use in the US by these ex-GIs. The grant of confidentiality enabled scientists to track a cohort of former service men, to collect urine to screen for drugs, and to conduct detailed interviews. The study documented an extremely low percentage of heroin use in the US by former users in Vietnam. The Certificate of Confidentiality has been applied to other studies in the addictions field, for example, to the studies that demonstrated the effectiveness of Methadone substitution therapy for heroin addicts, and it continues to be crucial to much clinical research in this area.

The AAMC strongly supports the argument that new federal legislation dealing with medical information privacy be preemptive of state privacy laws, with the exception of those state laws dealing with public health reporting requirements, which are well established, time tested and closely integrated with the nationwide data collection and evaluation activities of the Centers for Disease Control and Prevention. The Association recognizes that this recommendation is controversial, but argues that the support of medical research is a long-established and high priority of the federal government, and that there is therefore a compelling federal interest in ensuring that medical research is facilitated, and not hindered or blocked by a discoordinated patchwork of burdensome state privacy legislation. Much contemporary medical research, especially epidemiological and health services research, requires access to large, unbiased population samples encompassing many states. Accordingly, the Association recommends that any new federal confidentiality legisla-

tion should over-ride state laws to ensure consistent nation-wide governance of access to archival patient materials for research. The Association is troubled by legislation that allow states to enact tougher privacy laws or carve-out certain disease-specific state statutes from federal pre-emption. While acknowledging the sensitivity of this issue, we point out that many different diseases are considered especially sensitive by those who suffer from them and their advocates, and to single out a particular type of information, such as mental health records, for special protection opens a loophole in the intended federal preemption that the AAMC believes would prove very difficult to limit.

The impact of managed behavioral health care on mental health services has been profound. The health insurance programs of more than 162 million Americans requires them to access mental health services through these carve-out companies. The major companies offer services across the country. The positive side of managed behavioral health care is that it has made parity of health care coverage for mental illness a realistic option. In addition, the companies have been able to amass a great deal of information on the mental health services being provided to the US population. On the down side, controversies abound regarding the quality of care in some managed behavioral health care programs. Health services researchers have a great opportunity and responsibility to help the American public to assess the quality of mental health services in these programs. This is not an issue that can be stopped at a state line. It is critical that managed behavioral health care companies be encouraged to work with the health services research community to assess quality of treatment outcomes, and that federal law pre-empt state privacy laws that would make this impossible.

The AAMC commends this Subcommittee for convening this hearing to address the need for confidentiality legislation and the efforts of Chairman Thomas and Rep. Cardin in crafting legislation that would enhance the security of medical records. The Association urges Congress to be mindful of the fact that the facilitation of biomedical, epidemiological and health services research is a compelling public priority that has served this nation well and offers bright promise for the future of human health. The AAMC strongly believes that the combination of statutory safeguards of the security of individually identifiable medical information, stiff penalties for violations, and the creation of special protections for medical information that is created in research and maintained in research databases, as we have suggested, make it unnecessary to elaborate new, burdensome and potentially chilling restrictions of access to medical information for purposes of retrospective non-interventional research.

Mrs. JOHNSON of Connecticut. Thank you very much.

Ms. Janlori Goldman, Director of Health Privacy Project for the Institute for Health Care Research and Policy. Nice to have you.

STATEMENT OF JANLORI GOLDMAN, DIRECTOR, HEALTH PRIVACY PROJECT, INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY, GEORGETOWN UNIVERSITY

Ms. GOLDMAN. Thank you for inviting me to testify here today. I appreciate it.

As you said, I am the Director of the Health Privacy Project at Georgetown University. I have been working on privacy and medical privacy issues for almost 13 years. What I would like to ask is that a revised version of my testimony, a neater version and one on disk, be allowed to be submitted for the record at a later date.

Mrs. JOHNSON of Connecticut. So ordered.

Ms. GOLDMAN. Thank you.

When I started the health privacy project a year and a half ago, I tried to position health privacy issues in a way that is a little bit different than how we tended to look at it in the past, to see protecting privacy as a critical goal to improving the quality of care in this country and access to care. We have tended to view these as values in conflict, and what we have found in some of our recent

research is that protecting privacy is critical to improving health care in this country and in opening doors to access.

In a recent survey that came out in January it was documented that one out of every six people in this country withdraw from fully participating in their own health care because they are afraid that their records will not be protected, so they don't fully disclose to their doctors, they leave information out. Sometimes they pay out of pocket to avoid having to file a claim or they don't seek care at all. So the quality of their care is undermined in those circumstances, and the information that is available downstream for public health and research is also undermined.

So I truly believe that we need to enact strong privacy legislation in order to give the public trust and confidence that this Nation's health care system will protect their privacy.

You are all well aware Congress has imposed on itself a deadline of August 21 to enact comprehensive legislation or the Secretary will issue regulations. When we started the Project, we tried to identify what is missing in the debate, what contribution can we make, and we decided that we would bring together the diverse stakeholders in the debate, the health plans, doctors, ethicists, mental health advocates, those representing people with AIDS and others, to say can we reach outside of the glare of the legislative spotlight, can we reach some common ground on a set of best principles for health privacy.

I had the privilege of working with Dr. Paul Clayton on that working group, and I included for you a copy of the working group's principles. I want to just highlight—we released this report last week, so we are just in time for the deadline—just a few of the key findings that we made.

We want to reverse the status quo and encourage people to use nonidentifiable data wherever they can, and to put in some real protections for individuals by having authorization requirements that are more meaningful than we heard about in the first panel, and to provide some oversight, some accountability for all research that is conducted in this country, not just the research that receives Federal funds and is covered by the common rule.

We were able to reach that common ground, and I think we have a lot to be proud of, and I hope that Congress will look and see if there is some guidance that you can find in this report as you move forward.

The second thing that we did, which we just released this morning and which has already been referred to by Congressman Cardin, is a report that is a comprehensive survey of the 50 State health privacy laws. That has never been available until today. And so when the question was asked earlier, well, do you comply with the 50 State laws, the truth is no one has known what they are. So today we released this report.

We have a summary of every State's law. You can look at your State of Connecticut, you can look at your State of Wisconsin and say what protections are provided to our citizens. And so when you are looking at this issue of preemption, which is one of the most controversial issues in the debate, you can say, what would be the impact on my State's law? What has my State done in moving forward to protect privacy?

Now, one of the things that we found in our State report, which I think is very important, the State law in this area is not simple, and it is not easy to find, which is why it took us so long and so many people to put this together. There is a lot of law, and it exists in the nooks and crannies of the States' code. There are very few examples, although Wisconsin is a shining exception, of comprehensive law. There are very few States that have enacted comprehensive health privacy law. They tend to legislate by entity. They might have restrictions on hospitals, health plans or doctors, but they don't tend to take a very comprehensive view. But what the States have done in a very, I think, responsive and responsible way, is to enact condition-specific rules. So for people, for instance, who want to seek genetic testing, for people with mental illness or communicable disease, the cancer registries and other kinds of disease registries, the States have been very responsive to protecting the needs of their citizens in those areas. We need to be cautious and look at those laws before we talk about creating a Federal ceiling.

What we also found is that some of the State laws are weak and some are strong, but they are for the most part very detailed and nuanced. I want to make a final point about the State laws. When we talk about uniformity, and this is the big discussion we are all having, how do we create uniformity. I think we all agreed that in this complex, health care environment with managed care and integrated health data networks, we all need uniformity to have good quality care in this country. The question is if we set the bar high enough at the Federal level, in other words, if we enact strong enough protections at the Federal level so that we don't have to worry about wiping out stronger laws that already exist at the State level, we don't have to worry about passing or enacting a Federal ceiling, because we will have done the best that we can do to create a baseline of protections for people in this country.

I think we want to be very careful and respect what the States have already done. The States have been very responsive. We don't want to tie the hands of the State in being able to respond to future public health threats. Many of the State laws on the books were enacted to respond to a particular public health threat or a public health concern. Again, the number one barrier to people receiving genetic testing is they are afraid of how that information will be used by somebody else, in employment, in insurance, so the States are moving forward to protect, to enact protections, to encourage people to get these critical tests that can help improve their care, so they have been able to respond to these concerns. We need to be mindful of the regulatory powers of the State and the details of the State law. So I just suggest some caution. The State report, by its title suggests there is an uneven terrain in the States, but I don't want to suggest it is an unimportant terrain. The States have done a lot of good in this area.

In conclusion, we should ensure that a Federal law does not weaken or erode the critical protections that already exist at the State level. Consumers have come to rely on those State laws for whatever protections do exist in the absence of a Federal law. If we do, we will jeopardize their health care and we might undermine their trust in public health and research. We should do our

best to make that floor as high a level of baseline protections as possible.

Thank you very much.

[The prepared statement follows:]

Statement of Janlori Goldman, Director, Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University

Chairman Thomas and Members of the Subcommittee:

Thank you for the opportunity to testify before you today on the issue of health privacy. I am Janlori Goldman, Director of the Health Privacy Project at Georgetown University's Institute for Health Care Research and Policy. In the past week, the Project has issued two reports on health privacy, which we hope will make a significant contribution to the ongoing policy initiatives. We include as our testimony today the top findings and executive summaries of these reports. The full text of both reports is available on our website at www.healthprivacy.org.

Your continued attention to health privacy is greatly appreciated, and we look forward to working with you, as you, and the rest of the Congress, move forward to meet the August deadline for enacting comprehensive health privacy legislation.

BEST PRINCIPLES FOR HEALTH PRIVACY

Executive Summary

Privacy and confidentiality have long been recognized as essential elements of the doctor-patient relationship. Also essential to optimal care is the compilation of a complete medical record. But that same record is used for a wide variety of purposes—including insurance functions, coordination of care, and research. The longstanding friction between these two goals—patient privacy and access to information for legitimate purposes—has been heightened by the transition to electronic health information and a push toward integrated information in support of integrated health care delivery and health data networks. While these developments are intended to improve health care, they also raise many questions about the role of privacy in the health care environment.

Recent polls demonstrate that the public has significant concern about the lack of privacy protection for their medical records and that it can impact how they engage with health care providers. In order to protect their privacy, some patients lie or withhold information from their providers; pay out-of-pocket for care; see multiple providers to avoid the creation of a consolidated record; or sometimes avoid care altogether. Such "privacy-protective" behavior can compromise both individual care and public health initiatives.

The public has some reason to be concerned. Today, there is little consistency in approaches to patient confidentiality and no national standards or policies on patient confidentiality. The 1996 Health Insurance Portability and Accountability Act provides that if Congress fails to enact comprehensive health privacy legislation by August 1999, the Secretary of Health and Human Services must issue regulations. Therefore, either through legislation, government regulation, or self-regulation, there will be significant developments with regard to health privacy in the next two years.

What has been missing from the debate is a consensus document that offers policy recommendations regarding how best to protect patient confidentiality. To fill this void, the Health Privacy Project, with funding from the Robert Wood Johnson Foundation, created the Health Privacy Working Group in June 1998. Its mission was to achieve common ground on "best principles" for health privacy, while identifying a range of options for putting those principles into practice. The Working Group is comprised of diverse stakeholders, including: disability and mental health advocates; health plans; providers; employers; standards and accreditation representatives; and experts in public health, medical ethics, information systems, and health policy.

The Working Group spent the past year crafting a consensus document that reflects "best principles" for health privacy. This report outlines the 11 principles to which the Working Group agreed and details the rationale behind the recommendations.

The principles represent significant compromises between Working Group members and should be seen as a framework that aims to accommodate the various information needs of diverse interest groups. The principles are designed to establish a baseline of protections that should be considered when implementing comprehensive patient privacy policies and practices.

The Working Group adopted the following 11 principles. Because these principles are intended to establish a comprehensive framework, they should be read and implemented as a whole.

1. For all uses and disclosures of health information, health care organizations should remove personal identifiers to the fullest extent possible, consistent with maintaining the usefulness of the information.

Generally, the use and disclosure of information that does not identify individuals does not compromise patient confidentiality. As such, the use and disclosure of non-identifiable health information should "fall outside" the scope of policies that govern personally-identifiable health information. Health care organizations will need to take into consideration the practicality and cost of using and disclosing non-identifiable information. Ultimately, through the creation and use of non-identifiable health information, more people can have more information, without compromising patient confidentiality.

2. Privacy protections should follow the data.

All recipients of health information should be bound by all the protections and limitations attached to the data at the initial point of collection. Recipients of health information can use or disclose personally-identifiable health information only within the limits of existing authorizations. Any further uses or disclosures require specific, voluntary patient authorization.

3. An individual should have the right to access his or her own health information and the right to supplement such information.

All patients should be allowed to copy their records and to supplement them if necessary. But supplementation should not be implied to mean "deletion" or "alteration" of the medical record. Furthermore, data holders may charge a reasonable fee for copying the records, but they cannot refuse inspection of the records simply because they are owed money by the individual requesting inspection.

In certain cases, patients may be denied access to their medical records. Such instances include if the disclosure could endanger the life or physical safety of an individual; if the information identifies a confidential source; if the information was compiled in connection with a fraud or criminal investigation that is not yet complete; or if the information was collected as part of a clinical trial that is not yet complete and the patient was notified in advance about his or her rights to access information.

4. Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.

The notice should tell the patient how information will be collected and compiled, how the collecting organization will use or disclose the information, what information the patient can inspect and copy, steps the patient can take to limit access, and any consequences the patient may face by refusing to authorize disclosure of information.

5. Health care organizations should implement security safeguards for the storage, use, and disclosure of health information.

Security safeguards consistent with the Secretary's standards, whether technological or administrative, should be developed to protect health information from unauthorized use or disclosure and should be appropriate for use with electronic and paper records. Any safeguards should recognize the trade-off between availability and confidentiality and should be tailored to meet needs as organizations adopt more sophisticated technologies.

6. Personally identifiable health information should not be disclosed without patient authorization, except in limited circumstances. Health care organizations should provide patients with certain choices about the use and disclosure of their health information.

Patient authorization should be obtained prior to disclosure of any health information. But, at the same time, some patient information needs to be shared for treatment, payment, and core business functions. With this in mind, the Working Group recommends a two-tiered approach to patient authorization.

The authorization structure allows for a health care organization to obtain a single, one-time authorization for core activities that are considered necessary or routine. These activities—identified as Tier One—are directly tied to treatment, payment and necessary business functions in keeping with medical ethics. The health care organization may condition the delivery of care, or payment for care upon re-

ceiving authorization for these activities, which can be obtained at the point of enrollment or at the time of treatment.

Any activities that fall outside this core group (sometimes commonly referred to as uses) must be authorized separately by the patient and fall under Tier Two authorization. The patient can refuse authorization for these activities without facing any adverse consequences. Activities in this category include, but are not limited to:

- purposes of marketing;
- disclosure of psychotherapy notes;
- disclosure of personally identifiable information to an employer, except where necessary to provide or pay for care;
- disclosure of personally identifiable health information outside the health care treatment entity that collected the information, if other tier one authorizations do not apply; and
- disclosure of personally identifiable health information, if adequate notice has not been given at the point of the initial authorization.

The Working Group identified a limited number of circumstances in which personally-identifiable health information may be disclosed without patient authorization. These include:

- when information is required by law, such as for public health reporting;
- for oversight purposes, such as in fraud and abuse investigations;
- when compelled by a court order or warrant; and
- for research, as described in Principle 8 below.

7. Health care organizations should establish policies and review procedures regarding the collection, use, and disclosure of health information.

An organization's confidentiality policies and procedures should be coherent, tying together authorization requirements, notice given to patients, safeguards, and procedures for accessing personally identifiable health information. Organizations should also establish review processes that ensure a degree of accountability for decisions about the use and disclosure of personally identifiable health information. During such a process organizations might, for example, wish to determine routine procedures and special procedures for some areas of health care where medical information is considered highly sensitive to the patient.

8. Health care organizations should use an objective and balanced process to review the use and disclosure of personally identifiable health information for research.

For some areas of research, it is not always practical to obtain informed consent and in some cases, a consent requirement could bias results. Recognizing this, the Working Group advises that patient authorization should not always be required for research. However, any waivers of informed consent should only be granted through an objective and balanced process.

Currently, any federally funded research is subject to the "Common Rule," where an Institutional Review Board (IRB) is required to make a determination about the need for informed consent. An IRB can choose to give a researcher access to personally identifiable health information with or without informed consent. But some research falls outside the scope of federal regulations. In such circumstances, health care organizations should use a balanced and objective process before granting researchers access to personally-identifiable health information.

9. Health care organizations should not disclose personally identifiable health information to law enforcement officials, absent a compulsory legal process, such as a warrant or court order.

Federal privacy laws generally require that some form of compulsory legal process, based on a standard of proof, be presented in order to disclose to law enforcement officers. Law enforcement access to health information should be held to similar standards. In some instances, however, government officials may access health information with legal process for the purposes of health care oversight. In these instances, the information obtained should not be used against the individual in an action unrelated to the oversight or enforcement of law nor should the information be re-disclosed, including to another law enforcement agency, except in conformance with the privacy protections that have attached to the data.

10. Health privacy protections should be implemented in such a way as to enhance existing laws prohibiting discrimination.

Currently, there are state and federal laws that prohibit discrimination on the basis of a person's health status in areas such as employment or insurance underwriting. Confidentiality policies should be implemented in such a way as to enhance and complement these protections. In effect, privacy can serve as the first line of

defense against discrimination, creating a more comprehensive framework of protection.

11. Strong and effective remedies for violations of privacy protections should be established.

Remedies should be available for internal and external violations of confidentiality. Health care organizations should also establish appropriate employee training, sanctions, and disciplinary measures for employees and contractors who violate confidentiality policies.

The 11 principles outlined above focus on information gathered in the context of providing patient care and are written to establish a broad framework for the use and disclosure of health information. Although the Working Group recognizes that the need for privacy protections in other areas is no less urgent, this consensus document does not address the following areas:

- special considerations about the needs of minors;
- information that locates an individual in a particular health care organization (sometimes referred to as "directory information");
- information provided to spouses, dependents and other next of kin;
- public health reporting;
- fraud and abuse investigations; and
- the appropriate relationship between state and federal law.

These 11 principles are designed to serve as a baseline for establishing patient privacy protections. While we all agree that health information, used in the right hands and with the right safeguards, can lead to improved health and advances in research, this information should not be used with disregard for patient privacy. Patients need to know that adequate protections are in place to protect their health information. Our hope is that these principles will go a long way towards establishing appropriate protections and, in the process, help build public trust and confidence in our health care system.

THE STATE OF HEALTH PRIVACY: AN UNEVEN TERRAIN

Preface

Eighteen months ago, the Health Privacy Project launched an initiative to compile and publish a comprehensive survey of state health privacy statutes. As word spread that we had undertaken this effort, we heard two distinct messages, often delivered by the same people in the same breath: First, "Nothing like this exists." Second, "Are you crazy? Do you have any idea what you are getting into?" Over the past year and a half, we have come to appreciate both the importance of this effort, and the near impossibility of the task.

At the outset, it is important to say what this report is, and what it is not. The State of Health Privacy includes a summary of each state's major statutes related to the confidentiality of personal health information. The survey is specifically and exclusively a survey of statutes, not laws. This distinction is important: we did not research or include regulations, or common law, both of which ultimately must be understood in order to appreciate the full range of protections at the state level.

The survey is not exhaustive—there are many more statutes that address the confidentiality of health information. The summaries speak most directly to the use and disclosure of information gathered and shared in the context of providing and paying for health care. In particular, the condition-specific requirements are meant to be illustrative; we did not do an exhaustive search for mandatory reporting requirements or specific conditions.

Throughout, keep in mind that medical information is used in many different settings, and for many different reasons. There are innumerable state laws that speak to the confidentiality of health information—such as laws on workers compensation, public health reporting, adoption records, birth and death records, motor vehicle requirements, minor's rights, and so on—that are not generally addressed in our summaries. For this reason, we have given four states—Florida, Maryland, New York, and Washington—a more exhaustive treatment that highlights the breadth and the depth of the state laws that relate to the confidentiality of health records.

To satisfy diligent scholars and the excessively curious, we augment the summaries with a comprehensive list of each health privacy-related law we discovered in the state. (Given the length of these lists, they are only available in the online edition at the Health Privacy Project's website: http://www.healthprivacy.org/resources.) We have also provided a number of overview documents that attempt to pull together the findings and provide a snapshot of how the states compare to each other.

This report is not perfect. We may have missed some laws. Laws may have been repealed or re-interpreted by the courts. Laws may take on a different meaning in their application than they do in the plain reading. States may have issued regulations implementing their laws that amplify, diminish, or otherwise affect the law's impact. However, we determined that you-the reader-would benefit from the timely publication of this report, and would not be offended by our asking your indulgence for what we did not have the time or the resources to accomplish. In fact, we ask your assistance—if you discover a major statute we have overlooked, or if you find we mis-characterize a law, or if there is anything else you would like to contribute to enhance the accuracy and completeness of The State of Health Privacy, contact us. Your input is appreciated.

Finally, and most importantly, this survey is part of a larger body of work undertaken by the Health Privacy Project. Throughout, we have tried to maintain a sense the ultimate goal: to protect the privacy of people's health information.

In the health care arena, maintaining the confidentiality of medical information and communications has been an essential element of the relationship between doctors and their patients. Increasingly, however, major changes in health care—such as the rise of managed care, the development of electronic health information networks, and reform efforts to improve individual and community health—all depend on accumulation of and access to complete and reliable patient data.

Protecting privacy and improving health and access to health care are values that have long been viewed as in conflict. Consumer advocates often view public health and research initiatives as threats to individual privacy, whereas public health officials and researchers may treat privacy as a barrier to improving health. In fact, the converse is true—protecting privacy and promoting health are values that must go hand-in-hand.

Without trust that the personal, sensitive information that they share with their doctors will be handled with some degree of confidentiality, patients will not fully participate in their own health care.

The consequences of people not fully participating in their own care are quite troubling, for individual patients as well as the larger community. For instance, incomplete or inaccurate information can hamper a doctor's ability to accurately diagnose and treat a patient, inadvertently placing a person at risk for undetected and untreated conditions. In turn, if doctors are receiving incomplete, inaccurate information, the data they disclose for payment, research, public health reporting, and outcome analysis will be unreliable. Ultimately, information that lacks integrity at the front end will lack integrity as it moves through the health care system. Thus, protecting patient privacy is integral both to improving individual care and to the success of public health initiatives and quality of care.

There is no doubt that the public is deeply concerned about the lack of privacy in the health care environment. A survey released by the California Health Care Foundation in January 1999 found that "public distrust of private and government health insurers to keep personal information confidential is pervasive. No more than about a third of U.S. adults say they trust health plans (35%) and government programs like Medicare (33%) to maintain confidentiality all or most of the time." The consequences of such distrust—real or perceived—are significant. The Foundation's survey identified that:

• One in every five people believe their health information has been used or disclosed inappropriately.

• One of six people engage in some form of "privacy-protective" behavior when they seek, receive, or pay for health care in this country. Such behavior includes paying out of pocket for care; intentionally seeing multiple providers to avoid the creation of a consolidated record; giving inaccurate or incomplete information on a medical history; asking a doctor to not write down the health problem or record a less serious or embarrassing condition; and even not seeking care to avoid disclosure to an employer.

Currently, there is no comprehensive federal law protecting the privacy of people's medical records. Congress has acknowledged that such a law should be passed and imposed a deadline on itself to do so by August 1999. If Congress fails to meet the deadline, the Secretary of Health and Human Services is required to issue regulations by February 2000.

Health privacy is not a new issue to the U.S. Congress. Each year over the past decade as debate has resumed over how to best craft a health privacy law, the question is inevitably raised, "What have the states done? What are the state health privacy laws? What will be the impact on the states of any federal preemption of state law? What negative and positive models exist for us to learn from?" For the most part, these questions have gone unanswered. Until now, no comprehensive compilation of state health privacy existed.

Bear in mind as you read this report that, in the absence of a comprehensive federal health privacy law, the limited privacy protections people currently enjoy have been put in place by state legislatures. The terrain of state health privacy law may be uneven, but that shaky ground plays a significant role.

Executive Summary

There is no comprehensive federal law that protects the privacy of people's health information. The U.S. Congress is moving ahead to meet a self-imposed deadline to enact a broad health privacy statue by August 1999. If the deadline is not met, the Secretary of Health and Human Services must issue regulations by February 2000. At this time, people must rely on whatever health privacy protections are built into their state's statutes.

As the congressional debate over health privacy heats up, there is a question that is always asked but—until now—impossible to answer. "What state laws exist in this area? How have states responded to the health privacy needs of their citizens?"

This report is the first-ever comprehensive 50-state survey of health privacy statutes. In our experience, the hallmarks of researching state health privacy laws have been that: 1) nothing is simple; and 2) nothing is predictable. In the process of researching, analyzing, and summarizing the statutes, we reached a number of conclusions and made a few surprising discoveries. But in many more ways, the states defy categorization.

State laws relating to health privacy have been enacted at different points in time, over many years, to address a wide variety of uses and public health concerns. One must approach each state on its own terms and attempt to understand the protections as a unique whole within the state. In striving for precision and nuance, our labels of state laws are accompanied by qualifiers and explanations.

Laws relating to health privacy can be found in nearly every nook and cranny of a state's statutes—in obvious and obscure sections of a state's code, buried in regulations, developed in case law, and detailed in licensing rules. Florida, for example, has more than 60 statutes that address health privacy, and it is not unique.

A number of initial observations emerge from the state summaries:

• States legislate and regulate health privacy by entity.

There is little mystery about why state health privacy laws are so extensive, vast, and detailed: the statutes reflect the diverse users of health information. Consider the following four types of users: physicians, schools, insurers, and state agencies. Each has a specific function in the state and a legal and regulatory structure specific to their roles. Thus, the statutory requirements for how they handle medical information are different.

To understand what confidentiality protections do exist at the state level, one must first begin by examining the laws applying to the different entities that collect, use, maintain, and distribute health information. Even states that attempt to handle health privacy in a comprehensive fashion ultimately establish unique rules for different entities. In looking at a state's laws and determining what kind of privacy protections exist, one must always ask, "Who's holding the data?" and "What is the medical condition at issue?"

The end result of this legislating by entity is that state laws—with a few notable exceptions—do not extend comprehensive protections to people's medical records. Thus, a state statute may impose privacy rules on hospitals but not dentists. The state may restrict the use and disclosure of information derived from a genetic test but not information obtained in a routine physical. Or just the opposite may be true in a neighboring state.

The cumulative effect of these various statutes might appear erratic, but so many of the laws that do exist provide meaningful protections for consumers and speak to the specific needs of the organizations and citizens of the state. For instance, a nursing home may have different information needs than a public hospital, and state laws attempt to accommodate these differences.

• The vast majority of state statutes were never intended to be comprehensive.

Virtually every state has some law aimed at the confidentiality of patient, but very few states have anything approaching a comprehensive health privacy law. Two notable exceptions are Rhode Island and Wisconsin, each of which has comprehensive health privacy laws. Many states have health privacy laws governing certain health care entities, such as hospitals or clinics, but no privacy protections regulating health plans and HMOs.

State confidentiality requirements are part and parcel of larger statutes that provide consumer protections or regulate persons or entities. Many of the statutes, for example, are imbedded within licensing requirements. In this context, the provider is required to maintain health information in confidence in order to obtain and maintain a license to practice from the state. One must read all of the statutes to-

gether in order to glean an understanding of how health information is protected as it moves between persons and entities.

• An ethical duty to maintain confidentiality is often assumed.

Most states appear to presume an ethical duty on the part of health care providers to keep information confidential. Many statutes, for instance, do not explicitly impose a duty of confidentiality, but they do stipulate a penalty for breaching patient confidentiality. It seems that in these instances, the states did not see a need to legislate the ethical duty. Unfortunately, the users of health information have extended well beyond those who may be bound by a professional codes of ethics.

• State laws have not kept pace with changes in health care delivery and technology.

Most state laws do not reflect the dramatic changes in the health care environment or the dramatic changes in information technology. Today, for instance, the majority of health care is not delivered by physicians. Integrated delivery systems (such as HMOs and provider networks) and the establishment of statewide health information databases have created new demands for data that push well beyond the limits originally anticipated by the states. The variety of people and entities collecting, receiving and using health information has also extended far beyond the health care environment. A physician, for example, may be obligated to report a person with epilepsy to the Department of Motor Vehicles, which in turn may revoke a driver's license.

Therefore, in many ways, the state laws defy summarization—they are detailed, specific, and intricate. Nevertheless, we have attempted to bring some coherence to this report. The summaries are arranged in four broad categories: Patient Right of Access, Restrictions on Disclosure, Privilege and Condition-specific Requirements. Our major findings in each category are listed below.

Key Findings

Patient Access

States vary widely in the rights they grant to patients to receive and copy their own medical records. Some states have no statutory right of access such as Kansas and North Dakota. Three states—Alabama, Idaho, and New Mexico—and the District of Columbia only have a statutory right for patients to access their own mental health records.

On the opposite end of the continuum, a few states—such as Connecticut and Minnesota—grant access to records maintained by nearly all of the potential sources of patient data, i.e. government agencies and entities, hospitals, physicians, insurers, schools, and even non-traditional health care providers such as natureopaths. Maine and South Dakota, for example, have cast a particularly wide net with respect to providing access to records maintained by health care providers by using broad definitions that anticipate future users and holders of medical information, such as those performing in vitro fertilization and blood banks.

Most states fall somewhere in the middle of these two extremes. Forty-four states provide some right of access, but this figure is a bit misleading. The right of access quickly breaks down:

• 33 states provide a right of access to hospital records;
• 13 states provide a right of access to HMO records; and
• 16 states provide a right of access to insurance records.

Many additional statutes cover specific providers—such as physicians, psychiatrists, and pharmacists. However limited the right, the impact of providing the right should not be underestimated. For example, in response to the public's desire to utilize alternative sources for contact lenses, Colorado and other states require optometrists to disclose prescriptions to their patients.

All state statutes that grant people a right to see and copy their own medical records limit that right with a set of exceptions. The most common exception is that a patient can be refused access to his or her own medical record if the record holder believes that the release of the information could endanger the life and safety of the subject of the information or another person.

Many states have also granted patients the right to amend or correct their medical information, particularly when the records are held by insurance companies. In Illinois, New Jersey and Ohio, for example, the statute includes a detailed procedure for resolving a patient's challenge to the accuracy or completeness of the record. Where the provider and the patient disagree, for example, the patient may be able to insert a statement of his or her position in the record.

Most states allow a person or entity to charge patients for copies of their medical record. Some states specify a cost in the statute—in Kentucky, for example, a health care provider or hospital must provide a patient with a free copy of their medical

record. A patient may be charged for additional copies, but not more than $1 per page. Other states require that the fee be waived if the patient is contesting an adverse underwriting decision. The most common approach is to stipulate that an entity may charge a "reasonable" fee.

Restrictions on Disclosure

States vary widely in terms of the restrictions or prohibitions they impose on disclosures of medical records and medical information. The restrictions tend to be triggered in two instances: by the entity holding the data, and the kind of information being held.

For the most part, the state statutes prohibit a person or entity from disclosing information unless certain conditions are met. The most notable impact of this approach is that it may limit the actual protections afforded the data. Once the information is disclosed, it may or may not be afforded the same protections by the receiving entity. For instance, the state laws may not place limits on the re-disclosure patient data, or the receiving entity may not be under any legal obligation to adhere the privacy rules imposed on the disclosing entity.

In comparison, a few states—such as Wisconsin and Rhode Island—have statutes that prohibit medical information from being disclosed, regardless of the entity holding the record.

Overall, the most common restriction found in state statute is that patient authorization must be secured prior to health information being disclosed. Some states specify the format and content of the authorization form in statute. Many states allow patients to revoke authorizations.

At the same time, these statutes all specify numerous exceptions to this general rule in which a person or entity may disclose information without patient authorization. The most common instances include: for purposes of treatment; to secure payment for healthcare; for auditing; and for quality assurance activities. Most statutes allow access to patient data for research purposes, without any patient notification or authorization. (See later discussion on research.)

Also of note is that some states do prohibit the re-disclosure of medical information. In such instances, an entity that receives medical information is prohibited from re-disclosing the information unless a separate authorization is secured, or the disclosure is in keeping with the statutory requirements. Montana has stated that although it is state public policy that a patient's interest in the proper use of health care information survives, the state is not going to statutorily regulate disclosures because a person' expectation of privacy changes when the information is held by a non-health care provider.

Privileges

A common myth is that the doctor-patient privilege prohibits health care providers from sharing information about their patients. The truth is the law of privilege is a rule of evidence and quite limited in scope. Privilege applies to a patient's (or provider's) right to keep certain communications confidential in a legal proceeding.

We have included a survey of states' statutory privileges for two reasons: 1) to date, all of the proposed federal health privacy legislation leaves state privilege law intact; and 2) many states' statutes governing the confidentiality of health care information maintained by HMOs provide that an HMO is entitled to claim any statutory privilege against disclosure that the provider of the information is entitled to claim. Thus, in order to understand what privilege an HMO might be able to exercise, it is necessary to know what statutory privileges exist.

A common misconception about the physician-patient privilege is that it is a general prohibition against a health care provider sharing information about his or her patients. However, it is important to recognize that in legal terms, there is a distinction between "privilege" and "confidential." The law of privilege is generally seen as a rule of evidence which is limited in scope. It allows a patient in a legal or quasi legal proceeding to refuse to disclose and to prevent others from disclosing certain confidential information (usually communications) obtained during the course of diagnosis and treatment. In contrast, a health care provider's duty of confidentiality to her patients, arising from a code of ethics, by regulation, or otherwise, is a broader duty not to disclose to the public information obtained in a professional capacity.

That being said, it must be noted that even legal professionals often use the terms interchangeably. We have attempted to note where a state has worded its statutory privilege in such a way as to extend it beyond a legal or quasi legal proceeding.

It must be emphasized that this is a summary of statutory rules of privilege. Many more providers and entities may be covered by a state's common law privilege. The summaries do not include a discussion of when privilege may be waived.

State law is detailed and voluminous on this subject, and we chose simply to indicate to whom the statutory privilege applies.

Condition-specific Requirements

Nearly all states have laws that impose condition-specific privacy requirements, most often to shield people with mental illness, communicable diseases, cancer, and other sensitive, stigmatized illnesses from broad disclosures. Many of these laws were passed to respond to public fear that certain health information would be widely disclosed and used to deny them benefits or could result in other harm. Where this fear acted as a barrier to seeking health care, treatment, or counseling, states have moved to bolster public trust and confidence in the health care system by enacting heightened privacy rules in these specific areas. The protections tend to attach to the information at the point of collection, before the information is disclosed. These requirements may, for example, direct a provider, hospital, or laboratory to obtain a particular kind of authorization from the patient or more stringently restrict disclosure.

In some circumstances, the condition-specific requirements allow for greater disclosure of the information. Some mental health statutes, for example, explicitly allow family members to access the mental health records of a family member who has been committed. Other statutes allow employers to share medical information about an employee if it affects the performance of her job.

Most of the condition-specific requirements that exist at the state level, however, were enacted hand-in-hand with mandatory reporting laws. While the summaries note the protections afforded the data, it is important not to lose sight of the fact that these privacy laws were enacted on the backend of laws requiring doctors and other health care providers to report to state officials identifiable patient data related to certain illnesses and conditions. Clearly, state lawmakers viewed such privacy protections as a necessary balm to quiet public fears of the government developing health information databases on vulnerable citizens. Our inclusion of the public health reporting requirements and related privacy protections are not comprehensive, but we point out that many states' reporting requirements are aimed beyond communicable or infectious diseases. Many states collect health information to study costs, outcomes, and quality—all of which rely on extensive patient data. In turn, there is a great demand—often answered in the affirmative—for access to this data.

All states have laws designed to control the spread of contagious diseases, which include requirements that named individuals with particular illnesses or conditions be reported to health authorities. Again, in the vast majority of these condition-specific requirements, the privacy protections are linked to the mandatory reporting requirements. In such instances, the confidentiality requirements and protections only apply to the agency collecting the data. Many states, for example, require providers to report birth defects to the state's registry. The statute then limits how the registry can use and disclose the information. These protections, however, do not apply to any other entity holding the same information—such as a provider, hospital or insurance company.

Remedies and Penalties

Most state health privacy statutes contain some form of remedies and penalties that are triggered by violations of the law. Commonly found are private right of action provisions granting people the ability to bring lawsuits when the statute has been violated, without first having to meet any additional standard of proof, i.e. that the violation was willful or intentional. It is enough that the law was violated. A full range of damages, remedies, and attorney's fees and costs are usually available, however the monetary damages are often set quite low. In some cases, these statutory remedies may be construed as exclusive, thereby barring people from raising other claims, such as privacy torts or other common law claims.

Government-maintained Records

Across the board, records held by government agencies and officials are treated differently—and are usually more protected—than the medical information collected and held by the private sector. In some instances, the medical records held by the government are the only records protected in statute. In effect, a state statute may impose confidentiality requirements only on public hospitals, leaving people who are treated in private hospitals without the same legal safeguards. In Oregon, for example, the statutory prohibitions on disclosure, including authorizations, apply only to public providers of health care. Private health care providers are simply "encouraged, but not required to adopt voluntary guidelines limiting the disclosure of medical records..."

Although this legal distinction—between public and private holders of medical information—is rooted in the constitutional principle that there must be limits on government action vis-a-vis the individual, it may not be particularly meaningful to health care consumers. Therefore, privacy protections have been extended in a number of federal and state privacy statutes to restrict the private sector's collection and use of personal information.

Research

Again, there is little uniformity in how state statutes regulate researcher access to people's medical information. The vast majority of laws, however, do allow researchers broad access to patient records. As the laws apply to private entities, researcher access is almost always built in as an exception to a statute's patient authorization requirements. What limits do exist usually speak only to specific information—such as genetic information or HIV/AIDS information.

On the other hand, researcher access to patient data held by government entities, i.e., agencies, registries, is in some instances more detailed. Some registries, for example, have strict conditions that must be met before researchers can access data and may require that personal identifiers be removed before a researcher can access information. Laws applying to government entities are also more likely to prohibit researchers from re-disclosing patient data.

Conclusion

Again, there is no comprehensive federal law protecting the privacy of people's medical records. Congress has acknowledged that such a law should be passed and imposed a deadline on itself to do so by August 1999. If Congress fails to meet the deadline, the Secretary of Health and Human Services is required to issue regulations by February 2000. We hope these reports are useful to you as you move forward. We are available to work with you.

The Health Privacy Working Group Members: Dr. Bernard Lo, University of California-San Francisco; Paul Clayton, Columbia Pesbyterian Medical Center; Jeff Crowley, National Association of People with AIDS; John Glaser, Partners Health Care System, Inc.; Nan Hunter, Brooklyn Law School; Shannah Koss, IBM; Chris Koyanagi, Bazelon Center for Mental Health Law; John Nielsen, Intermountain Healthcare; Linda Shelton, National Committee for Quality Assurance; and Margaret VanAmringe, Joint Commission on Accreditation of Healthcare Organizations.

As this report documents, there is little probability that any federal law could match the breadth and scope of the existing state laws. As such, any federal law that fully preempted state law would eliminate for consumers some of the rights and protections they currently enjoy and disrupt current state legal and regulatory structures. Here's why——

• States have been the first to respond to concerns about health privacy and they have enacted many strong protections.

State health privacy statutes cover a broad range of entities and, not surprisingly, are both weak and strong. In terms of broad consumer protections, one can identify many significant gaps and weaknesses in most state statutes: such as a limited right for a patient to access his or her own medical record; little ability for patients to limit disclosure of their medical records; and little recourse when the laws are violated.

On the other hand, state laws enacted in response to a particular public concern, or a public health threat—such as in the areas of mental illness, communicable disease, cancer, and genetic testing—are often strong, detailed, and aimed at the states' unique experiences with their citizens.

• State laws address a level of detail not considered in any of the federal proposals.

The importance of the detail in state health privacy law should not be underestimated. Because the states legislate by entity, they are often able to craft laws that speak to the unique needs of the patient population and the information needs of particular entities. An HMO, for example, has very different needs than a family planning clinic.

• State law is extensive—it is impossible to predict the full impact of full federal preemption.

Most importantly, it is almost impossible to predict the full impact of federal preemption on state laws relating to health privacy. Remember that these summaries are only the tip of the iceberg in terms of relevant state statutes. Many more laws govern areas such as adoption, workers compensation, public health reporting, civil, judicial and administrative procedures, fraud and abuse, and law enforcement access.

There is widespread consensus that a federal law could help to provide significant new protections and to establish some basic rules about the use and disclosure of health information. However, until this point, the policy debate about preemption tended to be based on rhetoric, not fact. There is a large body of law before us now. While many of the facts are reassuring, it does not lend itself to easy answers.

A significant challenge is before us. There is no doubt that such a comprehensive federal health privacy law could be beneficial in many ways. But while a federal law could substantially benefit people by establishing a baseline of consumer protections, a federal law that ignored the significant role states have played in protecting health information could disrupt the legal and regulatory structures at the state level and, in turn, some of the protections currently afforded to consumers.

Our hope is that this report will serve as the factual basis upon which to proceed, providing us with a true opportunity to move beyond the rhetoric that has so far defined this debate.

THE PREEMPTION DEBATE

At the national level, there is an ongoing debate over how a future federal health privacy law should relate to existing and future stronger state laws. Passage of any federal law will necessarily preempt weaker state laws. But will Congress choose to establish a federal "floor" above which states would be free to enact greater protections? Or will the federal law fully preempt state laws by creating a "ceiling," thus eliminating both weaker and stronger state laws and preventing the passage of future stronger state laws?

We must begin with the obvious: there is a large body of state law that will be impacted by *any* federal law. Many of these laws were passed over many years, and they cover significant ground. Out of necessity, the states have moved forward in recent years to pass health privacy laws to fill a vacuum that might otherwise be addressed in a federal law—such as in the areas of genetic testing, prescription records, HMO records, and integrated databases. A couple of states—such as Rhode Island and Wisconsin—have even passed fairly comprehensive laws.

Thus far, the preemption debate has played out as follows. Proponents of the full preemption of state law argue that a one-size-fits-all national standard is necessary to conduct health care activities across state lines. Advocates for a federal floor argue that states must be free to enact stronger protections to shield its most vulnerable citizens from stigma and discrimination, and encourage them to seek care without fear of reprisals.

But this debate must be about much more. As our research shows, the states' health privacy protections are deeply integrated into powers traditionally held by the states: licensing, public health, and police powers. As such, it would be unwise—and, in fact, unprecedented—for the federal law to fully preempt state law. At a minimum, the states must be free to enact greater protections for its citizens, to regulate health care entities, and to conduct vital public health functions.

Health Care Organizations Already Comply With 50 State Laws

Consider the state of affairs today: health care entities that do a great deal of business across state lines are currently required to comply with fifty different business across state lines are currently required to comply with fifty different state laws. The interplay between state and federal laws is not unique to the health care environment. In the context of other complex, interstate activities, Congress has addressed the interplay between state and federal laws, such as in the Right to Financial Privacy Act, the Fair Credit Reporting Act, and the Electronic Communications Privacy Act, which regulate the banking, credit, and communications industries. In enacting these laws, Congress left the states free to enact more protective laws as they see fit.

Some preemption supporters have expressed the fear that states will pass laws tat are too privacy protective, thereby interfering with important health-related activities. Our research documents that states have been quick to take corrective action to respond to the concerns of health plans, researchers, and others when they have 'gone too far.' In two instances in which a state health privacy statute was deemed to interfere with vital health care functions, states have moved quickly to amend their laws. Minnesota, for example, amended its law relating to researcher access to medical records after hearing objections from health care organizations in the state. More recently, Maine repealed a health privacy law after objections on the part of press and family members and later enacted a more limited statute.

Many states are considering pending health privacy bills in an attempt to fill the gap created by the absence of a federal health privacy law. In other contexts, however, the momentum behind such state initiatives drops significantly following the

passage of comprehensive federal legislation. After passage, state activity is likely to reflect the standards set out in the federal law, thereby increasing uniformity.

One of the more surprising—and potentially unifying—findings of this report is the most state laws are weaker than the standards proposed in many of the federal now under consideration. Therefore, a federal law may provide a substantial degree of uniformity simply by preempting weaker state laws, However, policymakers should be cautions not to interfere with the states' vital and established public health and regulatory mechanisms.

State Laws Address a Level of Detail Not Considered in Any of the Federal Proposals

State health privacy laws address a level of detail not found in any of the federal proposals. For the most part, state health privacy laws are organized by entity, and the statutes include requirements and specifications explicitly related to that entity. There may be separate statutes governing many different entities: employers, nursing homes, health maintenance organizations, health and life insurers, psychiatrists, chiropractors, hospitals and insurers.

In addition, there are numerous policy issues traditionally acted on at the state level that include health privacy provisions. There include anti-discrimination laws, commitment proceedings for the mentally ill, adoption, foster care, mental health treatment, reproductive health, parental involvement, partner notification, and abuse and neglect.

In comparison, federal health privacy proposals have on the whole treated all health care organizations the same. The federal proposals would also establish—with a broad brush—general rules governing the use and disclosure of health information. These proposed Rules aim to address the vast majority of circumstances in which health information is used and disclosed, but they do not begin to approach the level of detail that has been imbedded in state law. For instance:

• In South Carolina a physician is expressly prohibited from selling medical records to someone other than a hospital or provider licensed by the state. Before a physician may sell medical records, he must publish a public notice of his intention to sell the records and of a patient's right to retrieve their records if they prefer that their records not be included in the sale.

• Maryland has an intricate statutory system for dealing with mental health records. The disclosure of mental health records is governed by the state's Confidentiality of Medical Records Act. One provision stipulates that mental health records may not be disclosed between health care providers unless a patient has received a current list of the participating providers and has signed a written agreement to participate in the client information system developed by the agency.

• In Florida, a minor may obtain treatment for sexually transmissible diseases without the consent to their parents or guardians. [Fla. Stat. Ann. § 384.30.] The fact of consultation, examination, and treatment of the minor is co0nfidential, not subject to the disclosure requirements of other statutes, and cannot be divulged in any direct or indirect manner except as authorized by statute, including sending a bill to the parent or guardian.

The level of detail illustrated above is not even contemplated by any of the current federal proposals, and regulating these specific and unique spheres is clearly not the intent of any of the federal proposals. If Congress decides to fully preempt state law, it will most likely eliminate significant consumer protections without replacing them with an equivalent degree of federal safeguards.

States are the First to Respond to Concerns About Privacy and Have Enacted Many Strong Protections

Based on our research, it appears that many state laws governing the broad agrees sought to be covered in the federal law—patient access to records, notice of information practices, patient authorizations for disclosure, remedies for violations of the law—are weaker than many of the federal proposals. Thus, a federal law that established a floor could provide uniformity, while raising the overall privacy protections for consumers.

However, it appears that even the strongest federal proposals would not set the bar as high as the condition-specific protections in certain state laws. Thus, a preemptive federal ceiling could cause the citizens of some states to actually forfeit the protections they are now guaranteed under their state laws. Again, states have enacted condition-specific protections in two main areas: 1) to provide back-end protection to information collected as part of a mandatory reporting requirement; and 2) to encourage people to seek care for conditions that are sensitive and for which there is a high risk of stigma and discrimination.

• Almost every state has enacted laws specific to HIV/AIDS. California, for example, has enacted laws, covering testing, reporting, partner notification, and dis-

covery. The results of an HIV/AIDS test may not be disclosed in a form that identifies an individual, without patient consent for each disclosure, except in very limited circumstances. For instance, a physician or local health officer may disclose HIV test results to the sex or needle-sharing partner of the patient without consent, but only after the patient refused or was unable to make the notification. The law also requires patient authorization in more circumstances than provided for under the Senate proposals. In California, an individual's health care provider may not disclose to another provider or health plan without written authorization, unless to a provider for the direct purposes of diagnosis, care, or treatment of the individual.

• Almost half the states now provide specific and strong protection for information derived from genetic information. In Georgia this information is considered to be strictly confidential and may be released only to the individual tested and to persons specifically authorized by such individual to receive the information. Any insurer that possesses information derived from genetic testing may not release the information to any third party without the explicit written consent of the individual tested.

• Every state has laws that establish rules particular to mental health information, covering a wide range of activities. In Massachusetts, for example, a psychologist needs a patient's written consent to disclose any confidential communications about the patient, including the fact that the patient is undergoing treatment. An HMO is prohibited from acquiring or disclosing any communication by a member to a psychotherapist arising out of the outpatient diagnosis or treatment of a mental or nervous condition without the express and informed written consent of the member. No such written consent may be made a condition of the receipt of such benefits or any other benefits for which the member is otherwise covered.

• Tennessee law stipulates that the state's Department of Health records on sexually transmitted diseases may not be released even under subpoena, court order, or other legal process, unless the court makes a specific finding concerning each of five criteria including: weighting probative value of the evidence against the individual's and public's interest in maintaining its confidentiality; and determining that the evidence is necessary to avoid substantial injustice to the party seeking it and either that the disclosure will not significantly harm the person whose records are at issue or that it would be substantially unfair as between the requesting party and the patient not to require disclosure.

Many states have laws similar to the ones cited above. Again, none of the federal proposals reach these levels of specific protection. Wiping out such laws could create a public health crisis, leaving people vulnerable by undoing protections that encourage people to seek testing, counseling, and treatment for a number of conditions.

It is Impossible to Predict the Full Impact of Full Federal Preemption. State Law is Extensive—a Fully Preemptive Federal Law Runs the Risk of Significant, Unintended Consequences.

Even a cursory glance at the state statutes reveals that laws relating to the confidentiality of medical information are found throughout state codes. Major statutes are found in the Civil Code, the Insurance Code, the Health and Safety Code, the Penal Code, and the Welfare and Institutions Code. The laws cover a wide range of activities including treatment, payment, insurance-related activities, peer review, research, and prescribing drugs. Most importantly, states have developed bodies of law around discrete issues that touch on the use of health information—such as anti-discrimination, worker's compensation, parental involvement, adoption, HIV/AIDS partner notification, and access by law enforcement, and even real estate.

It is nearly impossible to predict in advance the full impact of total preemption on state law and consumer protections. Some laws, for example, may be tied to larger anti-discrimination statutes. A fully preemptive federal law may inadvertently nullify the entire statute.

• For instance, A California law that prohibits insurers from discriminating on the basis of a person's "genetic characteristics that may, under some circumstances be associated with disability in that person or that person's offspring." The law includes a provision on authorization requirements for the disclosure of genetic information, which may open up the entire statute to preemption.

Overall, the states are best equipped to respond to new, unique, and inherently local challenges in health care and public health. It is impossible to predict what issues will require prompt attention in the future, but a preemptive federal law would prevent states from responding at all.

Conclusion

State health privacy statutes are both weak and strong. In terms of broad consumer protections, many gaps and weaknesses can be identified in most state stat-

utes—such as a limited right for a patient to access his or her own medical record; little ability for patients to limit disclosure of their medical records; and limited recourse available to people when the laws are violated.

On the other hand, state laws enacted in response to a specific and heightened public concern, or a public health treat—such as in the areas of mental illness, communicable disease, cancer, and genetic testing—are strong, detailed, and aimed at a state's experience with its own citizens.

The level of detail in state health privacy law should not be underestimated. Because the states legislate by entity, they are able to craft laws that speak to the unique needs of their citizens, both in terms of the patient population, and the information needs of particular entities. An HMO, for example, has very different information needs than a family planning clinic.

An urgency exists to pass a comprehensive federal law that protects the confidentiality of medical information, fueled in part by the congressionally-mandated deadline to do so and by escalating public anxiety over the lack of enforceable health privacy rules. There is widespread consensus that the federal government must act to protect the privacy of people's records. However, as this report documents, we must proceed with extreme caution in determining the appropriate relationship between any future federal law and existing and future state laws.

While a federal health privacy law could significantly benefit consumers by establishing a baseline of consumer protections, if not handled properly and with an eye to the existing state laws, a federal law could also significantly disrupt the regulatory and legal structure at the state level, thereby weakening or eliminating crucial consumer protections.

Bear in mind that these summaries are only the tip of the iceberg of the state statutes relating to health privacy. It is impossible to foresee all of the laws that would be affected by a preemptive federal law. This report is intended to be the beginning of a dialogue on preemption that is grounded in fact, not rhetoric and conjecture.

The challenge before us now is to examine the impact of the passage of any federal health law on the privacy rights of various state citizens. We must also rely on this compilation of state statutes as we address the federal proposals' impact on state public health and regulatory regimes. The State of Health Privacy takes the first step to answering many of these challenges before us by providing the empirical basis on which to do so.

Mrs. JOHNSON of Connecticut. Thank you very much. Mr. Thomas Jenkins, the Assistant General Counsel for Blue Cross Blue Shield of Nebraska, on behalf of Blue Cross Blue Shield Association.

STATEMENT OF TOM JENKINS, ASSISTANT GENERAL COUNSEL, BLUE CROSS AND BLUE SHIELD OF NEBRASKA, ON BEHALF OF THE BLUE CROSS AND BLUE SHIELD ASSOCIATION

Mr. JENKINS. I am Thomas J. Jenkins, Assistant General Counsel of Blue Cross and Blue Shield in Nebraska, testifying today on behalf of the Association. Thank you for the opportunity to testify.

Protection of the confidentiality of subscriber data is of paramount importance to us. As part of employee training at Blue Cross and Blue Shield in Nebraska, employees must sign a policy that stipulates confidentiality breaches may result in termination. While we believe that consumers must be assured that their records are kept confidential, we believe that Federal legislation must balance the need to safeguard medical records with the need for health plans to provide health care services efficiently.

Let me highlight four areas where certain proposals on the table now fail to achieve this balance.

Number one, new authorizations. One of the goals of Federal legislation is to guard against disclosure of personal data. Of course,

health plans must disclose personal data in order to administer health benefits.

Some bills accommodate this through a statutory authorization for data disclosure for treatment, payment or health care operations. Other legislation requires health plans to obtain new and multiple authorizations from all of their subscribers. This requires mailing authorization forms to each of our 550,000 subscribers, as well as developing new systems to track whether or not those authorizations have been returned.

Even after multiple mailings, some subscribers will never respond. The postage costs alone would be significant, but would pale in comparison to the personnel and system costs necessary to accommodate this authorization process.

Because of these proposals, we would be forced to cancel the coverage of subscribers who fail to return these authorizations because we could not process their claims without legal access to their personal data. We urge Members of Congress to adopt a statutory authorization as part of confidentiality legislation.

Number two, static definitions. The statutory authorization makes it imperative that the definition of health care operations include all the functions we now use to administer benefits, but most proposals incorporate a static definition. They do not allow for innovative services to be added.

This year another Blues plan adopted a new program called SARA, Systematic Analysis Review and Assistance. Every day their computer evaluates data to identify files that need further review. This program has improved the care of subscribers. For instance, a 60-year-old male had claims for Viagra as well as for nitrates. The combination of these two types of drugs has the potential to be fatal. The SARA program worked with his physician to resolve this conflict.

A 1-year-old child had 15 claims for emergency room visits in the past 18 months. The parents were referred to an asthma program. No further visits to the emergency room were required in the next 6 months after that.

If a prescriptive definition for health care operations had been legislated in, say, 1995, we could never have developed this program. I urge you, therefore, to assure any definition can accommodate innovation.

Third, inspection and copying. This problem involves provisions that would allow subscribers to inspect, copy and amend all information that is individually identifiable. Most data we obtain are administrative in nature. For example, the claims. We believe it is important to differentiate between these data which must be protected from the data which must be produced.

Under some proposals, we would have to produce even insignificant paper that may have a subscriber's name or identifying item on it, routine claim runs, and so forth. This would require us to redesign our computer systems and operations to centralize all data, an extremely expensive investment that would increase premiums. This absolute approach is not necessary. In my State a recent law limits the inspection rights to medical records held by providers. We urge Congress to limit inspection rights to actual medical records.

Fourth and final, the preemption of State law. We have had a lot of discussion of that today. We believe any Federal legislation should preempt State confidentiality rules. The patchwork of State privacy laws are especially difficult when viewed from the patient-provider perspective. For instance, if a patient's insurance is through an employer in New York City, but their physician is located in New Jersey and the patient lives in Pennsylvania, whose confidentiality laws apply? How does the provider know how to comply?

We urge Congress to provide a full preemption of State confidentiality laws.

Thank you again for the opportunity to testify today.

[The prepared statement follows:]

Statement of Tom Jenkins, Assistant General Counsel, Blue Cross and Blue Shield of Nebraska, on behalf of the Blue Cross and Blue Shield Association

Mr. Chairman and Members of the House Ways and Means Subcommittee on Health, I am Tom Jenkins, Assistant General Counsel of Blue Cross and Blue Shield of Nebraska, testifying today on behalf of the Blue Cross and Blue Shield Association. BCBSA represents 51 independent Blue Cross and Blue Shield Plans throughout the nation that together provide health coverage to 73 million Americans. Thank you for the opportunity to testify on efforts to protect the confidentiality of medical records. I want to especially thank you Chairman Thomas for your work and the extensive efforts of your staff regarding confidentiality and other key health care issues over the last few years.

During my testimony, I will discuss:

(I) the importance of confidentiality of medical records;

(II) general principles for confidentiality legislation; and

(III) key issues raised by pending confidentiality legislation. These include:

- requirements for new authorizations from all subscribers;
- a static definition of health care operations;
- provisions mandating inspection, copying and amendment of individually identifiable information by subscribers; and
- preemption of state law.

I. THE IMPORTANCE OF CONFIDENTIALITY OF MEDICAL RECORDS

Blue Cross Blue Shield of Nebraska covers 550,000 residents in Nebraska—or 1 out of 3 people in the state. We offer the choice of products that our customers demand—health maintenance organizations, preferred provider organizations, point of service products, as well as traditional indemnity coverage.

Protection of the confidentiality of subscriber and patient information is of paramount importance to Blue Cross and Blue Shield Plans. We believe that health plans should make every effort to guard this confidentiality and should put into place procedures and policies that facilitate this goal.

Since its inception, Blue Cross Blue Shield of Nebraska has had protections to safeguard the privacy of our subscribers. As part of training for all new employees, we emphasize the importance of the information with which they are entrusted to maintain and safeguard. Dissemination of confidential information is absolutely forbidden. Violation of confidentiality by an employee is grounds for disciplinary action or termination. Employees also are educated that it is completely inappropriate to share medical information with their fellow workers outside those whose direct function necessitates it.

As a health insurer, we require medical information to pay claims, guard against fraud and abuse, and manage health care coverage. Our employees must sign a confidentiality policy with Blue Cross Blue Shield of Nebraska that includes recognition of a disciplinary policy that enforces our code of conduct.

II. GENERAL PRINCIPLES FOR CONFIDENTIALITY LEGISLATION

While the Blue Cross and Blue Shield Association believes that consumers must be assured that their medical records are kept confidential, we believe that federal legislation must balance the need to safeguard medical records with the need for providers and health plans to provide and cover health care services efficiently.

Federal legislation should:

• Protect consumers: All subscribers and patients should be confident that their medical records are kept confidential.
• Be practical and simple: Federal confidentiality rules must be practical and straightforward, so that providers and health plans can adopt and implement them. Consumers' rights must be easily understood. Complex rules will only confuse and frustrate consumers, and could hamper implementation throughout the industry.
• Allow for innovation and flexibility: The delivery and financing of health care continues to evolve at an exponential rate as new technologies and therapies are introduced and as e-commerce revolutionizes the way health care entities conduct business. Legislation must assure that health plans and providers can continue to evolve and provide innovative benefits to consumers.
• Have an achievable implementation date: Considering the challenges that health plans already face in terms of systems changes and backlogs due to Y2K, it is imperative that federal confidentiality legislation have a workable, achievable effective date. We urge an effective date of plan years beginning on or after 2 years after promulgation of final regulations.
• Provide for uniformity: Given the complex and interstate nature of the way information flows in today's health care environment, and the increasingly integrated nature of our health care delivery system, we believe consistent rules across the country are critical to assuring uniform treatment of confidential information.
• Avoid excessive penalties: Congress should not impose a new private right of action allowing individuals to file lawsuits against health plans, providers, employers, and others. Unfortunately, it is subscribers who suffer most because premiums would ultimately be increased to cover the costs of frivolous lawsuits. Moreover, some employers, especially smaller employers, may view the increased liability as an unacceptable risk and drop their employer sponsored health coverage altogether.

III. Key Issues Raised By Pending Confidentiality Legislation

Many federal proposals addressing the issue of confidentiality fail to incorporate all of the above principles. I would like to highlight several of the key issues we have identified with pending legislation.

(a) Requirements For New Authorizations

One of the general premises of federal confidentiality legislation is to prohibit health providers and plans from inappropriately disclosing personal data. Of course, health plans must disclose personal data to doctors, hospitals, and others in order to administer health insurance benefits. Some legislators have tried to accommodate this need by including a "statutory authorization" for the disclosure of data for treatment, payment or health care operations. That is, personal data are legally allowed to be disclosed or used without a separate authorization from the individual if it is needed for treatment, payment or health plan operations. We support this approach because the statutory authorization serves all parties well—it allows health plans to provide the services for which their subscribers are paying premiums in an efficient manner.

Unfortunately, other confidentiality legislation requires health plans to obtain new and multiple authorizations from all of their subscribers and their families before data can be used for treatment, payment, and health care operations. This would require us to mail new authorization forms to our 550,000 subscribers as well as develop new computer systems to track whether or not authorizations have been returned.

Many subscribers already are inundated with "junk" mail and may inadvertently throw these authorization forms away. We may have to mail to our subscribers two, three or more times before successfully receiving the new signed authorizations. Some may never respond. The initial postage cost alone would be significant but would pale in comparison to the personnel and system costs necessary to accommodate the authorization process. Unfortunately, according to various bills, we would be forced to cancel the coverage of subscribers who failed to return these authorizations because we could not process their claims without legal access to their personal data. And this is just on the private side of our business.

Medicare provides another example of the extraordinary difficulties of complying with this rule. Medicare enrolls over 37 million individuals. Over half of the older population reports having at least one disability. Over 4.4 million have difficulty carrying out activities of daily living such as bathing, dressing, eating and getting around the house. And yet, many confidentiality bills would require these individuals to return a written authorization to Medicare before their benefits could continue. If for any reason this authorization was not returned, the payment process would have to be suspended while further attempts to obtain the needed authoriza-

tion were made. Ultimately, payments to providers would be slowed down, anti-fraud and abuse efforts would be impeded, and it could be nearly impossible to maintain an efficient system.

Similar issues are raised in the Medicaid program. The National Association of State Medicaid Directors recently reported to the Blue Cross and Blue Shield Association that the following issues complicate the dissemination of materials to Medicaid recipients:

- High turnover rates in the Medicaid program;
- Homelessness and frequent residence-changing;
- Illiteracy;
- Nursing home residence; and
- The fact that beneficiaries often overlook the numerous notices that they receive in the mail.

Whether or not our customers enroll with us through our private business, Medicare contracts, Medicaid, or other government programs (e.g., CHAMPUS, Federal Employees Program)—they all share a common expectation: their health data will be used to cover their health costs. Requirements for new authorizations would only anger customers who already abhor paperwork, increase the cost of their coverage, and disrupt the payment of claims.

We urge Members of Congress to adopt a statutory authorization as part of confidentiality legislation.

(b) Static Definition of Health Care Operations

As I mentioned previously, a "statutory" authorization would allow health plans to use patient data for the purpose of health plan operations. This elevates the importance of the definition of health plan operations, and makes it imperative that it encompass the many functions a health plan now uses to assure the quality and cost-effectiveness of benefits for subscribers. Our concern is that most legislative approaches incorporate a static definition of health care operations—a prescriptive list of operations as they currently exist. They do not allow for innovative services to be added. This could deprive consumers of important—yet to be developed—services in the future.

For instance, this year another Blue Plan adopted a new program called the Early Risk Management Program. So far, it covers about 100,000 of their enrollees. Every day, their computer program evaluates data on those enrollees to identify "triggers" that indicate a need for further review of that patient's record. Those triggers may be a certain prescription drug or another admission to the hospital. On average, about 60 patient records per day are pulled for review. If, based upon this review, a problem is suspected, the patient's physician is contacted. Through this early risk management program, they have been able to improve the care of subscribers. For instance:

- A 60 year-old male had claims indicating prescriptions for Viagra as well as nitrates. The combination of these two types of drugs has the potential to be fatal. When the treating physician was called, he was unaware that the patient had obtained a prescription for Viagra. He agreed to contact the patient and no further prescriptions for Viagra were filled.
- A one year-old child had 15 claims for emergency room visits in the past 18 months as well as office visit claims for asthma. The parents were referred to an asthma case management program including outreach and education. No further emergency room visits occurred in the next six months.
- A 49 year-old male had recent claims for abdominal pain with no apparent etiology. Drug claims also indicated the patient was taking Naproxen. The treating physician was contacted and the physician indicated that a prescription for Naproxen had been given some time ago. The physician suspected that the patient continued taking this drug after the original episode for which it was prescribed had ended—likely leading to the abdominal pain.

New technology has allowed us to provide this quality improvement and potentially life-saving service to customers. But this type of program was not possible—or even contemplated—several years ago. If a prescriptive definition for health care operations had been legislated in 1995, we could never have developed this program.

I want to reemphasize that the delivery and financing of health care continues to evolve at an exponential rate as new technologies and therapies are introduced and as e-commerce revolutionizes the way health care entities conduct business. We are concerned strict definitions of health care operations could limit health plans' roles as they seek to redefine themselves to meet consumer demands of the 21st century.

I urge Members of Congress to assure that any legislative definition of health care operations be fluid, and easily adjusted over time as innovative programs that benefit consumers are further developed.

(c) Inspection, Copying And Amendment Of Individually Identifiable Information By Subscribers

Another example of problematic pending confidentiality legislation involves provisions that would allow subscribers to inspect, copy and amend all information that is individually identifiable. BCBSA believes that patients should be allowed to inspect and copy their medical records. However, the vast majority of information that health plans maintain is administrative in nature (e.g., claims) and does not reflect actual patient medical records. We believe it is important to differentiate between what information must be protected from what information must be produced.

The way most proposals are currently written, virtually every piece of information in a health plan could be copied and amended. Moreover, how a health plan would be required to produce or provide access to data in an intelligible format is a crucial question to consider.

For example, under some legislative proposals, we would have to produce even insignificant paper that may have a subscriber's name or identifying feature on it—customer service telephone memos, recordings of conversations, internal audit memorandum, routine claim runs, etc. We have concerns that producing and providing access to all of this data would require health plans to redesign their computer systems and operations to centralize all Plan data—an extremely expensive investment. It is conceivable that we may also have to provide the subscriber access to our computer systems. But in order to accomplish this, we may have to provide a "translator" to teach the subscriber how to translate the coded information on the computer. And of course, we would have to design new systems that would prevent the consumer from accessing other subscriber files while reviewing their own.

All in all, these requirements would pose administrative costs that would be passed along to consumers in the form of higher premiums. And all to create absolute access to information that is unlikely to provide meaningful information to the vast majority of subscribers. This absolute approach is not necessary. For instance, in my state a recent law limits the inspection and copying rights to medical records held by providers. These records are those that provide the basis for our operations, and are of the most interest to patients.

We urge Congress to limit inspection, copying, and amendment rights to actual medical records when adopting federal legislation.

(d) Preemption of State Law

Finally, we believe any federal confidentiality legislation should preempt state confidentiality rules. The intent of the Health Insurance Portability and Accountability Act (HIPAA) administrative simplification provisions was to simplify health insurance claims processes, reduce paperwork, and decrease administrative costs through wider use of automation and electronic data interchange (EDI). Federal standardization of confidentiality rules is essential to the integrity of that information. Lack of federal preemption may lead to the unintended consequence of a decline in use of EDI since it would be extremely difficult to create a computerized system that could assure compliance with conflicting state laws. Further, lack of federal preemption leads to higher compliance costs, which would ultimately be passed onto consumers in the form of higher premiums.

The patchwork of state privacy laws are particularly difficult when viewed from the patient and provider perspective. For instance, if a patient's insurance is through an employer in New York City, but their physician is located in New Jersey and the patient lives in Pennsylvania—whose confidentiality laws apply to the consumer? And how does the provider know how to comply?

Given the complex and interstate nature of the way information flows in today's health care environment, and the increasingly integrated nature of our health care delivery system, we believe consistent rules across the country are critical to assuring uniform treatment of confidential information.

We urge Congress to provide a full preemption of state confidentiality laws.

IV. CONCLUSION

The issues raised by confidentiality legislation are complex and fraught with potential unintended consequences. During my testimony, I have highlighted only a few of the difficult issues with this important subject. This Committee—and Congress—must successfully navigate through a labyrinth of land mines in order to enact confidentiality legislation that provides practical, strong protections for con-

sumers without disrupting the basic day-to-day services of a health plan and raising unnecessary administrative costs.

On behalf of all Blue Plans, I would like to offer our assistance to you as you continue upon this important endeavor.

Thank you again for the opportunity to testify.

Mrs. JOHNSON of Connecticut. Thank you very much. I appreciate the panel's input. I very much appreciate examples of how review of patient records has improved the quality of care.

Ms. Goldman, you said something that was really very interesting. First of all, your review of State law would be very helpful to us and I thank you for that.

Ms. GOLDMAN. You are welcome.

Mrs. JOHNSON of Connecticut. It is not surprising to me that the laws are fragmented and complex.

Given that fact, if we pass a national comprehensive law, it seems to me that we should allow a certain amount of time for States to conform to that law. I would not be opposed to States then applying for a waiver to have some additional law. But I am very concerned about going through all of the difficulty of coming to agreement on national standards, which I think is going to be very difficult. You can tell from my questioning, I am pretty conflicted about it. I don't know as much about it as my Chairman. It is not an area on which I spent a lot of time, but it is an area in which I have a lot of anxiety, and people I represent have a lot of anxiety.

So it is going to be hard to do this. It does seem to me that it is an area in which we do need uniformity. So I think everybody needs to sort of think about how do we deal with the States on this and if we do this right, there shouldn't be too many areas in which there is legitimate need to be different.

Ms. GOLDMAN. May I give an example of where there might be? Some may find that this is oversimplifying, but I want to just try to take this massive tome and create a simple conclusion.

In the broad areas that Congress is seeking to regulate in the health privacy area, the right of access, limits on disclosure, law enforcement, restrictions on law enforcement access, and those broad areas, the State law tends to be weaker than what many of the Federal proposals put forth.

So any Federal law that passes would create a floor. The question is where is that floor? The higher the floor, the higher the bar; the more State laws that are weaker will be eliminated and the greater the uniformity. In many ways there is an incentive on Congress if you are looking to develop uniformity to set that bar as high as possible because you will create significant uniformity given the state of the State laws.

However, in these, as I pointed out, these condition-specific areas, the protections that are on the back end of the cancer registries or other disease registries, where there is mandatory reporting requirements, but they are there for research purposes and the State has then enacted confidentiality protections to prevent redisclosure, or in the HIV/AIDS area, in a number of States there are very specific and detailed limits on the collection and use of

communicable disease information, again to encourage people to get testing, counseling and treatment.

The Federal proposals contemplate that level of detail and they tend not to be condition-specific. They tend to cover broad entities in the health care area and broad information that is identifiable health information.

So I would just suggest a great deal of caution about creating a totally preemptive approach at the national level, because there will be State laws that I think will be more protective than what we are able to come to consensus on here at the national level, because there will have to be a great deal of consensus and compromise necessary. Also States, because of their unique circumstances and needs of their citizens, have enacted particular kinds of rules in very, as I said, narrow areas.

Given that many in the industry: and the health plans, hospitals, doctors, right now have to comply with 50 different laws, that is their obligation now, we will greatly simplify that with a floor, with the greater simplification where we set that floor.

Mrs. JOHNSON of Connecticut. Would you all agree that the rules should be the same for HCVA as for private plans and for all providers and all State agencies?

Mr. CLAYTON. Yes. The problem is now there are no laws in many areas. We desperately need some laws. Where I lived in New York, we saw people from Connecticut and New Jersey; and if you build a computer program that has to look and see whether this person is from New Jersey before you can display their medication list, and have to look and see if they are from Connecticut before you can look at their problem list, people will be used to treating someone, and then when they don't see problems on the problem list, they may make mistakes in their judgments. When they use an information system, it has to be uniform.

As we start going to telemedicine, which will erase all political boundaries in terms of where things get done, then the preemption issue becomes even more difficult. I would just point out, even though Janlori is one of my friends, that her opinion on preemption was not one of the conclusions of the working group, that that is her personal opinion, and the working group did not reach that conclusion.

Dr. SMITH. When you limit research to just within a particular State because that is the only place you can get permission to do that research, you have a tremendous problem with generalizability. In other words, is it generalizable to other sections of the country, are there enough patients with that disorder or that particular issue within that particular State. So the idea of being able to move beyond State boundaries is very important. In order to have an informed health policy, this not only relates to specific diseases, but it relates to the economics of health care, it relates to how we improve our health care system, it relates to how we pay for it, how we monitor it. It is a very broad issue, and that is why we need a strong Federal law.

Mr. JENKINS. I think the truth may be also that the patchwork of laws may appear to be stronger in some instances as related there, but that may be a theoretical protection only if the laws are such patchwork that it is difficult to discern them, and that a

strong national framework would, in practice, be actually stronger, even though an editor or writer of an article like that might find it had been a reduction.

Mrs. JOHNSON of Connecticut. My understanding is the administration has not recommended overriding State law, just creating a floor. Do all of you agree that is the right thing?

Mr. JENKINS. No, I don't. I think it is an area where we are so fluid as a nation now in this health care area, that we need a set of rules that is standardized and we need to be able to follow them.

Mr. CLAYTON. I would, however, agree with Janlori, at least one idea, and I am thinking on my feet now. When a State mandates a certain data collection they are doing as a State, they might be able to have rules that pertain to that database.

What we are against is the State regulating the use of health care information in the normal operation of delivering health care; if there were a certain database that was required just in one State, there could certainly be a law concerning that State-mandated database, but not one that is in the normal operation of delivering health care.

So you might, following up on their suggestion, exempt specific types of databases, but not the ones that a physician or a nurse would be using in her general practice.

Mrs. JOHNSON of Connecticut. Would you differentiate between patient-identified information and nonidentified information?

Mr. CLAYTON. We definitely should differentiate and use, according to the need, legitimate need, for when it has to be identified.

Mrs. JOHNSON of Connecticut. Mr. Kleczka.

Mr. KLECZKA. Mr. Jenkins, does your organization support a Patients' Bill of Rights that covers all health consumers in the country, or only those consumers that the Federal Government has control of or regulation over?

Mr. JENKINS. We support rules that apply to the private plans, as well as the government plans, yes, sir.

Mr. KLECZKA. So you would support a Patients' Bill of Rights covering all 150-plus health care consumers, not only the ERISA plan consumers?

Mr. JENKINS. I am not sure of the position of the association on that. I better defer in speaking.

Mr. KLECZKA. I am trying to see if you share my problem with inconsistency on States rights. That is what I am trying to ascertain.

Mr. JENKINS. I think Mr. Thomas pointed out there are situations where, and I agree with his statement, there are situations where a full preemption is appropriate.

Mr. KLECZKA. I know your position on privacy legislation. I am asking your position on the Patients' Bill of Rights. There is a controversy in the Senate over whether or not to have the States control plans through their insurance commissioners' officers, and only have Congress deal with the federally controlled plans for the Patients' Bill of Rights.

Mr. JENKINS. My Association didn't take a position on that.

Mr. KLECZKA. I think you have a note coming forward on that.

Mr. JENKINS. On the Patients' Bill of Rights, the association supported the ERISA plan's approach that the Senate took. That is a note from the association staff.

Mr. KLECZKA. That indicates to me that on managed care reform you are letting the States govern. When it comes to health care privacy, the States don't know what they are doing and we should preempt them and the almighty Fed should regulate.

Mr. JENKINS. I don't think it is a matter of them not having the knowledge. There are good people who are on different sides of this issue at various points and decisions can and must be made.

Mr. KLECZKA. As a former State legislator and one from a State which has some exemplary protections in the medical records area, I think State legislators and the Governor should have the right to provide and afford protection to any degree for their consumers. I don't think the national interests outweigh that to the extent which some of you folks on this panel and some on the other panel would dictate.

Mr. JENKINS. I understand that, sir.

Mr. KLECZKA. Let me ask Dr. Clayton, who do you believe owns the medical records? Is it the health care provider or do you think that the patient is the owner of those records?

Mr. CLAYTON. Most of us in the field don't believe anybody owns the record. We are stewards. We act as the steward of that information, but nobody has really established who really owns it.

Mr. KLECZKA. So I as the health care patient have no direct ownership or claim to those records?

Mr. CLAYTON. I think what——.

Mr. KLECZKA. Even though I paid for them in part or at times in total, if I don't have insurance?

Mr. CLAYTON. What most laws that are being proposed say is that the patient has the right to look at those records, know that those records exist. That is fair information practice. Whether they can say they own them and then physically remove them from a doctor's office, I don't think anyone would maintain that is true.

Mr. KLECZKA. Maybe I don't own them, but I do have some control over them?

Mr. CLAYTON. If you own them, you can retrieve the property. But in this case you cannot retrieve it, which indicates to me you don't really have title. It has been a sticky issue that has a lot of case law, and most people agree that we are stewards of the records.

Mr. KLECZKA. You are the health care provider. I am the patient, OK. Do you think I have the right to make judgments as to who should see those records? Basically an opt in, not an opt out.

Mr. CLAYTON. I think if you wish to receive care and have someone pay for that care, you need to be able to let the people who are providing care have access to the information they need to provide that care.

Mr. KLECZKA. For specific purposes, not for any and every purpose.

Mr. CLAYTON. That is why I said in my statement that we strongly want to restrict the scope through policies. For example, an x-ray technician should have no information except the radiology results. A billing clerk who you call on the phone to complain,

"Why is my pharmacy bill so large?" needs to see what medications you are on. They may need to see what laboratory tests you took to answer your complaint about how large the bill was. But they don't need to see the results of those tests.

So we go through, we have at Columbian Presbyterian, three different categories of people and have listed them under what circumstances that person is in and what geographic location. In other words, if you are in the emergency room, a nurse could see more than if the nurse was at the nursing floor. So you restrict the scope of access to what is the legitimate need to know.

Mr. KLECZKA. That access is all pretty relevant to the course of business, and unless somebody is just a snoop, I don't see that much of a problem. The problem occurs when either the health care provider or some attendant group wants to give medical information to a third party or a fourth party, or when a doctor is selling patient information for a clinical drug trial where the physician receives rather substantial sums as payment for disseminating the names of patients.

Mr. CLAYTON. I think when you are using it for research, then it has to go through an accredited body that will determine need—so you don't just give information. Right now you can, because there is no law. If you make it law, then you will prescribe the ways in which we can divulge knowledge that information.

Mr. KLECZKA. Let me ask any of the panelists, what was your reaction to the drugstore chain in Washington selling lists of customers and the drugs they were prescribed to a competing drug manufacturer.

Mr. CLAYTON. Absolutely abhorrent.

Mr. KLECZKA. You can say it happened because of the absence of any medical privacy laws. What is your reaction to that?

Mr. CLAYTON. Should be illegal.

Mr. SMITH. In my opinion, it is immoral, unethical, and should be illegal.

Ms. GOLDMAN. One of the wonderful things about that case is right after it became public, that many drugstores were making this information available, people around the country went crazy. It was a tremendous outcry and uproar. There was article after article, and the chain drugstores that were responsible for this immediately eliminated the program. They didn't fix it, they didn't try to retool it in some way. They were doing it without patient knowledge, without their consent, and they eliminated the program. There are a couple of lawsuits ongoing on this right now.

Mr. JENKINS. The same feeling here.

Mr. KLECZKA. I don't think it is only a question of privacy for medical records, it is the entire question of privacy from the dissemination of Social Security numbers and medical records. We all know that Social Security number release leads to identity fraud. We have a Federal statute on that now. There is heightened public awareness in this whole issue. That is why when we discussed a banking bill, the big contentious issue on the floor of the House was the privacy provision in that bill.

Someone got up and said, we did this bill 2 years ago. Why wasn't privacy a big issue then? Because even though some of us were talking about it then, the public is now becoming more aware

of it. You take any poll and 85 to 95 percent of the people say it is a big issue.

During my last campaign, I did a poll. We asked people about Medicare and Social Security. We also asked about privacy, because I had an interest in it. That scored the highest of constituent interest in my district.

So, folks, if you think this is going to go away or we are going to be able to preempt States, I don't think we will get away with it. The public is irritated to the point now where politicians like yourselves should be listening.

I have to agree with the lady from Connecticut. Are we too late? Is the horse out of the barn? The Internet is there. I am frustrated, nervous and scared. We have to do something. We can't let it go on. It is going to get, as they say in some parts of the country, worser. We don't want it to get worser. We want it to get more better.

Mr. CLAYTON. Everybody strongly argued that there needs to be strong penalties and strong legislation. Not one of us would disagree with that.

Mr. KLECZKA. Thank you.

Mrs. JOHNSON of Connecticut. Thank you. I did want to just add for the record that the legislation for the patient protection that Mr. Thomas helped write and he and I both voted for did apply to all health plans, unlike the Senate bill. So I wouldn't want to have any misinformation out there on that score.

I do thank you all for your testimony. This is certainly a very difficult area and a very important one. We look forward to working with you and the administration to see if we can't get a bill that we can move through with some agreement on the difficult issues it poses.

Thank you.

[Whereupon, at 5:45 p.m., the hearing was adjourned.]

[Submissions for the record follow:]

AMERICAN ASSOCIATION OF
OCCUPATIONAL HEALTH NURSES
ATLANTA, GA 30341–4146

July 27, 1999

Committee on Ways and Means
U.S. House of Representatives
Subcommittee on Health
1102 Longworth House Office Building
Washington, D.C. 20515–6349

The American Association of Occupational Health Nurses, Inc. ("AAOHN") appreciates the opportunity to submit written testimony to the House Ways and Means Committee for the hearing record on the matter of confidentiality of personal health care information. Our primary purpose in submitting these comments is to urge Congress, in the strongest terms, to enact comprehensive medical records confidentiality legislation. We believe that for any medical record privacy bill to be truly meaningful, Congress must craft legislation that will ensure that all medical records are protected under the law regardless of the mode of payment or the setting where the health information is obtained or maintained.

AAOHN is the professional association for more than 12,000 occupational and environmental health nurses who provide on-the-job health care for the nation's workers. Occupational health nurses are the largest group of health care providers at the worksite. AAOHN has had a long-standing involvement in the confidentiality of health information debate and continues to work vigorously to ensure that employee medical records created and maintained at the worksite or any occupational health clinic are protected from improper disclosure.

Personal health information generated or maintained at the workplace or in connection with an individual's employment is as personal and sensitive as that collected in more traditionally thought of health care settings, and therefore, must be extended the same confidentiality protections. AAOHN trusts Congress recognizes the high degree of public concern about the very real potential for employment discrimination based on health information. Worksite health records frequently document medical and/or health surveillance activities, pre-job placement and fitness-to-work physical examinations, and employee assistance program assessments, as well as information collected through voluntary worksite wellness programs. Clearly, such information, if improperly disclosed, may be used in ways harmful to an individual's interests.

A. Balancing Individual Employee Privacy with Employers Needs

Indeed, AAOHN maintains that an individual employee's right to privacy must be balanced with employers' legitimate need for certain personal health information when considering fitness to work, workplace safety, workers' compensation benefits, disability job accommodations, or some employer-sponsored benefits. Employers must be permitted to fulfill their obligations under laws such as the Americans with Disabilities Act, the Family Medical Leave Act, and the Occupational Safety and Health Act, but employers *need not be granted* unfettered access to an employee's entire medical record to meet these legal requirements.

It is well documented that employers often inappropriately use employees' personal health information in making personnel decisions. For example, a 1996 research study by the University of Illinois revealed that at least one-third of the Fortune 500 company respondents admitted using employee medical records in making employment-related decisions.[1] Furthermore, AAOHN members can attest that they are often pressured by employers to release a worker's entire medical record or to divulge unnecessary personal health information of employees.[2]

B. Goals of Federal Privacy Legislation

Federal legislation can protect individual privacy and meet employers' legitimate needs for some employee protected health information ("PHI") if it includes safeguards that (1) limit the scope of individually identifiable PHI disclosed to an employer to that information necessary to answer a legitimate workplace health-related question and (2) create firewalls restricting access to employees' raw medical record by officers, management, and other employees responsible for personnel decision-making. It is essential to recognize that it is the health care provider, not an employer's administrative, human resource, or management personnel, who is the professional qualified to interpret medical data and determine what information is relevant for a particular health situation and should be disclosed. For example, AAOHN unequivocally believes that in cases of fitness-to-work examinations (e.g., medical surveillance records, health screening, return-to-work physical records) health care professionals should provide the employer with a written medical determination of an employee's health status based upon the medical record rather than handing the employer the actual record itself. Any employer entity would be hard-pressed to assert that its administrative, human resource or management personnel have the requisite qualifications to render a medical judgement as to the health of an employee based on their review of a medical record.

Limiting the amount of PHI an employer may learn about his or her employee is not a novel or untested approach. The "bloodborne pathogens" regulations issued by the Occupational Safety and Health Administration ("OHSA") explicitly require that such information must be kept confidential and "not disclosed or reported without the employee's express written consent to any person within or outside the workplace except when required by this section or as may required by law."[3] The law also narrows the extent of PHI provided to employers to that which is necessary to make a determination regarding work fitness. To this end, the regulation states that the "healthcare professional's written opinion . . .shall be limited to whether

---

[1] David F. Linowes, Privacy in the Workplace, University of Illinois at Urbana-Champaign, April 1996 (copy on file with AAOHN).

[2] See, e.g., Health Care Information Confidentiality: Hearings Before the Committee on Labor and Human Resources of the United States Senate, 105th Cong. (Feb. 26, 1998) (oral and written testimony of AAOHN).

[3] 29 C.F.R. Ch. XVII, § 1910.1030 (1998).

(appropriate treatment) is indicated for an employee, and if the employee has received such (appropriate treatment).[4]

C. AAOHN SUPPORT

Because of the importance of this issue, AAOHN will only support a federal medical records confidentiality bill that ensures worksite health records are recognized as PHI and that includes statutory language limiting intra-employer use and disclosure of PHI. To date, the only House bill including these types of provisions is H.R. 1941.[5] The "Medical Information Protection Act of 1999," H.R. 2470, introduced by Representative Greenwood does not cover worksite medical records. As originally drafted the Greenwood bill contained the same protections found in S. 881 introduced by Senator Bennett. Nevertheless, Representative Greenwood has stated for the record that these safeguards were inadvertently removed in the final version of his bill and that it is his intention to do all in his ability to add these protections to H.R. 2470.[6]

To ensure that worksite health records are recognized as PHI and that the special concerns surrounding health information generated or maintained at the workplace are covered, AAOHN believes that at a minimum the following amendments to H.R. 2470 are critical:

1. Add the term "*assessment*" to the definition of "health care" in section 2(6) to ensure that all types of health data generated at the worksite are "protected health information."

2. Amend the definition of "health plan" to *exclude* 42 U.S.C. § 300gg–91(c)(1)(G), "coverage for on-site medical clinics," from the benefits not included within the term "health plan"

3. Add new § 201(c):

(c) APPLICABILITY TO EMPLOYERS.—An employer may use an employee or agent to create, receive, or maintain protected health information in order to carry out an otherwise lawful activity, provided that

(i) disclosure of protected employee health information within the entity is compatible with the purpose for which the information was obtained and limited to the information necessary to accomplish the purpose of disclosure and (ii) the employer prohibits the release,

transfer or communication of the protected health information to officers, employees, or agents responsible for making work assignment decisions with respect to the subject of the information.

(1) The determination of what constitutes the information necessary to accomplish the purpose for which the information is obtained shall be made by a health care provider, except in situations involving payment or health plan operations undertaken by the employer.

AAOHN appreciates the opportunity to offer our comments regarding the importance of strong medical records privacy legislation to our nation's workers. In summary, effective federal privacy legislation must:

Define PHI broadly enough to include all medical records generated or maintained at the worksite or in connection with employment for purposes other than for treatment, payment, or health care operations;

Build barriers designed to restrict intra-entity disclosure in order to prevent management misuse of workers' health records without jeopardizing a company's ability to operate safely and efficiently; and

Recognize that the health care professional who creates or maintains worksite records is the appropriate person, not employer administrative, human resource, or management personnel, to determine whether a PHI disclosure is consistent with the purpose for which the information was lawfully obtained and limited to the minimum disclosure necessary to accomplish the purposes of the disclosure.

We urge Congress to keep these principles in mind when drafting any medical records privacy bill and look forward to working with Members of the Committee on Ways and Means on this important issue during the days ahead.

---

[4] *Id*.

[5] Senate bills S. 881 and S. 573 are notable for worksite protections.

[6] Legislative Hearing Regarding: H.R. 2470—Medical Information Protection and Research Enhancement Act of 1999 Before the Subcomm. on Health and Environment of the House Committee, 106th Cong. (July 15, 1999) (opening statement of Rep. Greenwood).

Statement of American Psychiatric Association

INTRODUCTION

APA, a medical specialty society representing 40,000 psychiatric physicians nationwide, appreciates the opportunity to provide a statement for this hearing. We believe patient privacy issues are one of the key issues before the Congress, and we greatly appreciate the Committee's interest in passing medical records privacy legislation.

As changes in technology and health care delivery have outpaced the statutory, common law, and other protections that traditionally have ensured patient confidentiality, the level of confidentiality enjoyed by patients has eroded dramatically. We must seize this valuable opportunity to protect and restore needed confidentiality protections.

But APA also urges you to craft legislation that will avoid the unintended consequences of many of the confidentiality bills pending before the Congress. Let's give a couple of real world examples of the impact of several of these bills on patients.

You go into your doctor's office, and the doctor gives you a comprehensive physical. He takes your blood and runs some lab tests. Sounds harmless enough. After all you never signed anything giving permission for your personal information to be broadly used and disclosed. You were never told your medical record would be broadly used, and nothing was sent to you. But it will be. Your medical records can be used for commercial research purposes. Without your consent or knowledge. Your age, sex, demographic information, psychiatric status and other information can be used for insurance underwriting and other broadly and vaguely defined health care operations purposes. Again without your consent or knowledge and even though aggregate, i.e. non-personally identifiable information would suffice. Even the banker reviewing your mortgage application can review your medical record without your consent or knowledge.

But certainly you think at least my employer is specifically prohibited from gaining access to this information. Not true. Several of the major proposals before the Congress lack the strong specific protections that are needed to insure that supervisory personnel cannot gain inappropriate access to your medical record. APA urges Committee members to avoid including any provisions in your legislation that would allow these disclosures to occur.

THE NEED FOR FEDERAL LEGISLATION

APA believes medical records confidentiality is one of the most important issues to come before the Committee this year. Our medical record, when it relates to conditions as varied as high blood pressure, communicable diseases, Alzheimer's disease, mental illness and substance abuse, domestic violence, sexual assault information, terminal illnesses, HIV/AIDS, cancer, eating disorders, sexual function or reproductive health issues, as well as many other conditions, is highly sensitive.

But whether or not we are affected by these illnesses, medical records privacy issues affect us all. Today's comprehensive medical assessments and wellness questionnaires can contain questions about patients' sexual behavior, social relationships, state of mind, and psychiatric status—even if patients are not receiving medical treatment relating to these issues. The forms can also contain extensive personal and financial information.

CONFIDENTIALITY IS A REQUIREMENT FOR HIGH QUALITY MEDICAL CARE

Common sense, the experience of physicians and patients, and research data all show that privacy is a critical component of quality health care. The sad fact is that the health care system has, on occasion, not earned the trust of patients, and many patients do not trust the system to keep their information confidential. In many cases, the result has been that physicians are not able to provide the best possible quality care nor reach many individuals in need of care.

Some patients refrain from seeking medical care or drop out of treatment in order to avoid any risk of disclosure. And some simply will not provide the full information necessary for successful treatment. At other times, physicians are approached by patients who ask us not to include certain information in their medical record

for fear that it will be indiscriminately used or disclosed. The result of all these behaviors resulting from patients' reasonable concerns is unfortunate. More patients do not receive needed care and medical records' data that we need for many purposes, such as outcomes research, is regrettably tainted in ways that we often cannot measure.

The solution is not to take short cuts that will further deprive patients of their rights. Instead, we must enact into law meaningful medical records privacy legislation based on the voluntary informed consent of patients and reliance upon the fullest possible use of deidentified and aggregate patient data. In this way the full advantages of patient privacy as well as the benefits of new medical technology can be harnessed.

Informed, voluntary, and non-coerced patient consent prior to the use and disclosure of medical records should be the foundation of medical records confidentiality legislation. As a general principle, we believe that the American Medical Association's position—that patient consent should be required for disclosure of information in the medical record with narrowly drawn and infrequent exceptions permitted for overriding public health purposes—is eminently reasonable.

THE SPECIAL SENSITIVITY OF MENTAL HEALTH INFORMATION AND THE U.S. SUPREME COURT'S JAFFEE DECISION

Patients often refrain from entering psychiatric treatment because of concerns about confidentiality. Not only do patients refrain from telling family members and close friends the information they share with their therapist, but some may not even tell their family members that they are receiving mental health treatment. Often, if the information were disclosed to a spouse or an employer it might jeopardize their marriage or employment. But even the privacy protection afforded to psychotherapy notes has eroded so much in recent years that many psychiatrists and other mental health professionals have stopped taking notes or take only very abbreviated notes. Without the very highest level of confidentiality, patients receiving mental health services will be less likely to enter treatment and less likely to remain in treatment. Worse yet, if confidentiality is not protected, the treatment patients receive will be less effective.

For these and other reasons, the U.S. Supreme Court recognized the special status of mental health information in its 1996 Jaffee v. Redmond decision and ruled that additional protections for mental health information are needed. The Court held that "Effective psychotherapy depends upon an atmosphere of confidence and trusta...disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment."

It is also worth recognizing that the extent of mental illness is widespread. According to the World Health Organization mental illnesses account for four out of ten of the leading causes of disability. APA urges members of this committee not only to protect the letter of the Jaffee decision but indeed to protect its spirit by including appropriate provisions in the legislation.

PROVISIONS NEEDED IN CONGRESSIONAL LEGISLATION

It is not our intention to provide a detailed analysis of each bill before Congress. Instead, APA would like to recommend several key provisions that we believe should guide the Committee in its deliberations.

Preemption. The most important medical records privacy issue before the Committee is to insure that stronger state medical records privacy laws are preserved and that states' ability to enact stronger medical records privacy laws are preserved. States have adopted valuable protections for patients, including laws limiting the disclosure of pharmacy records and laws blocking insurers' access to verbatim psychiatric notes. States are also actively considering numerous additional medical records proposals. In fact, the National Council of State Legislatures estimates that a total of 56 medical records confidentiality bills have passed through at least one chamber of a state legislature. We must not block states' efforts to protect citizens' medical privacy. We recommend that the Committee adopt a floor preemption approach, allowing stronger state medical records privacy laws to be preserved.

Consent. APA believes three principles should govern sections of the legislation concerning authorization and consent for disclosure. First, patients themselves should decide whether or not personal health information is disclosed. Consent before use and disclosure of medical records is critically important. This time-tested

approach should be preserved and strengthened in order to remain meaningful in the changing world of health care delivery. In general, whatever problems may now exist with confidentiality of health information are derived from our failure to observe this principle. No one is in a better position than patients themselves to identify sensitive information and to determine to whom it ought not to be revealed. Those who would alter this traditional approach have failed to justify such a radical change.

Second, identifiable personal health information should be released only when deidentified data is inadequate for the purpose at hand. Third, even when consent has been obtained, disclosure should be limited to the least amount of personal health information necessary for the purpose at hand. This is consistent with our recognition of the importance of protecting medical privacy.

These principles have implications for some of the major policy questions regarding authorization of disclosure. For patients to retain meaningful control over personal health information, prospective consent for routine disclosures of identifiable information should be largely limited to information needed for treatment and payment purposes. Other health care operations can usually be accomplished with deidentified data. With such a provision, a strong incentive will exist for the use and further enhancement of technology to perform a wide array of administrative functions.

Employee Protections. Millions and millions of Americans have great concern about the threat to confidentiality of their medical records due to employer access. Whether it is idle gossip by individuals with access to medical records, employer review of identifiable medical records data, or supervisors' inappropriate interest in the personal lives of their employees we must protect employees right to medical records privacy. Wouldn't most people want to decide if anyone in their company, not to mention their supervisor, would know if they obtained medical care from a psychiatrist, from a cardiologist, from an obstetrician/gynecologist, or from an oncologist? We believe that the strong, explicit protections are needed in this area.

Health Care Operations. APA is very concerned by the definition of "health care operations" in many of the bills before the Congress. Entities providing health care can use and disclose this information for "operations" purposes, i.e. many purposes not directly related to treating a patient or performing payment or reimbursement functions. Some of the terms that are used to define "operations" are quite vague and broad and could endanger patient privacy. Do we really want to permit patients to be terminated from their health care coverage because they don't want their personal records to be used for largely commercial functions that can be performed with aggregate data?

Needed Protections for Particularly Sensitive Medical Information. As indicated above, especially sensitive information, including mental health information needs to receive a very high level of protection. Indeed, the U.S. Supreme Court itself in its Jaffee decision recognized that additional privacy protections, above and beyond those afforded to other health information, are needed to insure effective psychiatric care. APA believes that in order to promote high quality medical care and patient privacy, the Congress should pass legislation that provides a level of protection high enough so that no class of information needs additional protections. However, in the event that the Congress proceeds with legislation that does not meet this test, strong additional privacy protections will clearly be needed for mental health information. Most important among these are protections to prevent access by insurers to verbatim psychiatric notes.

Self Pay. If individuals enter into a private contract with a physician and pay for those medical services out of their own pocket, it is difficult to understand why the government or a health plan should compel them to sign a form allowing their medical information to be broadly disclosed beyond the treatment team. Both liberal members of Congress who support personal privacy and members of Congress who support medical savings accounts and private contracting under Medicare should recognize the importance of strong self-pay provisions in medical records confidentiality legislation.

Protections from Overzealous Actions by Police. APA strongly believes that strong protections are required in this legislation including a requirement that law enforcement agents obtain judicial approval based on a probable cause standard before they are granted access to individually identifiable medical records. This approach would allow legitimate law enforcement investigations to proceed, without unnecessarily jeopardizing the privacy of sensitive health information. APA further believes that the Committee should incorporate a requirement that protected health information obtained pursuant to a court order for one investigation should not be used for any other investigation, except a secondary investigation arising out of or directly related to the original investigation. Finally, APA urges that law enforcement agen-

cies and officials should be subject to the same requirements for protecting individually identifiable health information obtained pursuant to a court order as apply to other recipients of protected health information, including health providers and payers.

Conclusion

As physicians, we take an oath first stated by Hippocrates that, "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick...I will keep silence thereon, counting such things to be as sacred secrets." In order to make sure that doctor-patient confidentiality continues to protect patients in the new millennium, I strongly urge the Committee to provide the highest possible level of confidentiality in your legislation.

We thank you for this opportunity and we look forward to working with the Committee on these important issues.

Statement of American Society of Health-System Pharmacists, Bethesda, MD

RE: CONFIDENTIALITY OF HEALTH INFORMATION

The American Society of Health-System Pharmacists (ASHP) supports responsible federal legislation to ensure that patients will be comfortable communicating fully with their pharmacists, physicians, and other members of the health care team, with the knowledge that their sensitive medical information will not be disclosed for illegitimate purposes. ASHP is the 30,000-member national professional association that represents pharmacists who practice in hospitals, health maintenance organizations, long-term care facilities, home care, and other components of health care systems.

ASHP believes the patient should have the right to access and review his/her medical records, and the ability to correct factual errors. Patients should also have the right to know who has access to their medical records, and authorize how their medical information is or will be used. ASHP recognizes that patients view certain medical information to be particularly sensitive. Nevertheless, ASHP believes all medical information is sensitive and should be treated with the utmost protection.

ASHP believes that pharmacists must have access to patient health records in order to provide quality care and ensure the safe use of medications. ASHP also believes that with access to the patient's health record comes the pharmacist's professional responsibility to safeguard the patient's rights to privacy and confidentiality. Within health systems, communication among all authorized health care practitioners is to be encouraged and in no way restricted, while ensuring patient confidentiality and privacy.

Pharmacists also participate extensively in many clinical trials involving drugs. ASHP believes that all clinical trial data must be recorded and stored in such a way that the subject's rights of privacy and confidentiality are protected. Adequate safeguards are already in place to protect a patient's health care information during the clinical trial process, including the storage and retrieval of data. As part of the established process of informed consent, patients receive a statement describing who will have access to patient identifiable information. This includes personnel from the study sponsor or the FDA for compliance purposes as well as institutional personnel who audit the information for quality or financial integrity.

ASHP believes that pharmacy residency and other training programs must implement policies and procedures to assure the confidentiality of patient medical records, while recognizing that pharmacy students and residents must have access to medical records in the course of their training.

ASHP believes that in cases where patient information is aggregated into a larger population and used for legitimate research and statistical measurement, there is no potential for a breach of patient confidentiality because it is not uniquely identifiable. Therefore, a specific authorization for access to this information by individual patients is unnecessary.

ASHP believes there should be a minimum standard adopted in federal law for protection of patient health information.

ASHP believes that strict governmental protections, with appropriate penalties for violations, must be in place to preclude the dissemination of patient-identifiable information outside of the health system (i.e., to an unauthorized third party) for any purposes that do not involve the direct provision of patient care or reimbursement. Health systems must have written policies and procedures in place to guard against

the unauthorized collection, use, or disclosure of protected health information. Strict governmental penalties including criminal sanctions for egregious violations should be considered. However, inadvertent infractions with no intent to harm should be subject to the health care organization's disciplinary process or civil penalties.

The American Society of Health-System Pharmacists is grateful for the opportunity to submit its views in writing on the subject of confidentiality of patient medical records. Questions regarding ASHP's policy in this area should be directed to Ellen C. Evans, Director, Federal Legislative Affairs, Government Affairs Division, 301–657–3000 ext. 1326.

Minneapolis, MN 55416
August 1, 1999

A.L. Singleton
Chief of Staff, Committee on Ways and Meams
U.S. House of Representatives
1102 Longworth House Office Building
Washington, DC 20515

Dear Mr. Singleton:

Confidentiality of my patient records is so important to me that should I feel it is no longer secure, I would think twice before receiving medical treatment for a serious illness. Thank you for giving me the opportunity to express my concerns to the July 20th hearing on medical confidentiality.

Patients and doctors have a special relationship requiring the divulging of confidential information that sometimes even the best of friends or family members do not share. There must be trust between the doctor and patient to allow for sharing what could be damaging information in order to allow timely and appropriate medical care.

For the integrity of this relationship and the health care system in general, it is important that patients have informed, voluntary consent prior to the sharing of information. The bills before the House and Senate do not protect this right. Rather, they would create a federal law allowing researchers, government agencies, law enforcement, and managed care organizations to enter my medical records at will. I am very uncomfortable with other people reviewing my personal medical records without my consent. They would also limit the right of my state legislators to enact stronger privacy legislation that Congress enacts.

As an American, I am entitled to certain rights, including the right of protection against unlawful search and seizure by others of my personal property. This includes personal information about myself. Also, the Nuremberg Code protects me against becoming an unwilling research subject.

Unconsented access to my medical records will not only violate my Constitutional rights as a citizen of the United States of America, it will leave me vulnerable to employment, insurance, and medical discrimination.

I urge you to truly protect my confidentiality by assuring patient consent prior to all medical record access. I also urge you to make the research consent form separate from the authorization to treat form and that it be made perfectly clear to the patient that their medical care is not in jeopardy should they elect NOT to authorize research on there medical records.

The doctor/patient relationship has eroded too much already with the induction of managed care into our medical community. As far as I'm concerned, medical privacy is the last bastion protecting that relationship and guaranteeing quality of care. When you destroy the sacred trust between a doctor and her patient, you compromise the physician's ability to practice medicine. Further, when patients no longer trust their physician, then the whole truth surrounding their medical condition will not be forthcoming and your research is tainted from the start.

Please pass REAL medical privacy legislation that is strong on protection for the patient, not on protection for the researcher. Otherwise, it is guaranteed that PRIVACY will have its day in court.

Thank you for your time.

Sincerely,

JOYCE E. ANDERSON
Citizen of the United States of America

Jefferson City, MO 65109
July 21, 1999

Mr. A. L. Singleton
Chief of Staff
Committee on Ways and Means
U.S. House of Representatives
1102 Longworth House Office Building
Washington, D.C. 20515

Dear Mr. Singleton:

Confidentiality of our patient records is very important to us. Thank you for giving us the opportunity to lend our comments to the July 20th hearing on medical confidentiality.

We would like to let you know what we, as private law-abiding citizens feel it is necessary for you to protect our medical records. Really protect it, not just say you tried to protect it, or that you thought you protected it.

First and foremost, no information should be released without our informed voluntary consent. There should be no coercion to sign. We should not be threatened with denial of care or additional expenses. In addition, it should be clearly stated on the consent form who the information will go to if we give our consent, and that we can limit the list. It should be clearly stated that consent is not required for us to receive treatment. It should also be clearly stated that we can revoke the consent at any time. The consent should be only for a limited period of time. We realize that if the doctor does the billing or if we have insurance pay the bill, we have to release information, but the information released should be limited to the claim for payment. It concerns us that HMOs and insurance companies are creating patient profiles with the information they receive. We think that is wrong. To get health care should not mean that we must give away all the intimate details of our life for someone else to track and sell.

We also want you to know that we believe that state legislatures should not be restricted to whatever law Congress enacts. We want our legislators to have the right to protect us to the greatest degree possible. Because the federal government's power is limited by the Constitution's according to the 10th Amendment, states are given the right to make decisions best for their own constituents. The federal government and Congress should not try to revoke it.

We have heard that the federal government and medical researchers believe that we should give up our right to privacy for the greater good and the public health of all. We also read that officials want us to let the police look at our records without our consent. Forcing us to display the intimate details of our life to the government and the police will not benefit our health. Given our ability to cross match data, we're not even sure that our unidentified data is unidentifiable, but we would have no problem letting our information be used if it was guaranteed that we could not be identified or found.

If it becomes law for the police, profit hungry researchers, and government to get into our records without our consent, we can assure you that we no longer will be forthright with our doctors. Just knowing the government is going to look willy-nilly through our medical records and create databases with our name and information on them will damage the relationship we have with our doctor. We're particularly concerned that whatever information is collected on us will be used against us. Maybe by insurance companies or employers, or regarding certain illnesses, by the people who hand out passports and drivers' licenses. These are not small issues.

There are few things more necessary to our freedom than our privacy. Imagine having to weigh every word and nuance when we go into the doctor. This could bring us into the black market for medical care or mental health. We want to trust our doctor, not fear him. He's supposed to be there to protect us, not hurt us. Every day, we see privacy being taken away. We would like you to help us protect our patient and privacy rights when you write this law. We don't care about the inconvenience it might make for health plans and researchers. We have ourselves to protect. Please keep us in mind.

Sincerely,

MATTHEW AND CARRIE BURCHAM

CONCERNED PARENTS FOR VACCINE SAFETY
ELY, NV
August 3, 1999

A.L. Singleton
Chief of Staff
Committee on Ways and Means
U.S. House of Representatives
1102 Longworth House Office Building
Washington, DC. 20515

Dear Members of Congress:

Please include these written comments as part of the official record.

I am writing to urge all of you to pass legislation which would require the written consent of all patients in order to access, share, or enter personal medical information into any database. We, Concerned Parents for Vaccine Safety, are extremely concerned about the possible invasion of medical privacy that is about to take place in the form of national databases, etc.

No one's personal medical information should be entered into ANY database without their written permission. Yet this is going on all across the country. In Washington state, infants are being entered into a database called Child Profile at birth without the parent's knowledge, much less consent. This is wrong. The government does not have the right to tag and track individuals for any purpose. Medical choices are exactly that, choices and are between the individual and the physician. These choices as well as other medical information should remain between those two parties and no one else without the explicit permission of the patient.

If something is not done soon, we can never go back. Once unique personal identifiers are assigned and once we open the flood gates and let anyone and everyone have access to private citizens' medical information, the sky is the limit for abuse, punishment, and discrimination. Please allow the American public to keep what little freedom and privacy they have left. Do not allow the creation of unique personal identifiers. Do not allow access to personal health information to every Tom, Dick and Harry. Do not allow American citizens to have their last little bit of privacy violated. Do not allow American citizens to be tagged and tracked like a herd of cattle. There is no good reason to allow such things to happen. We are all individuals with hopes, dreams and lives. We deserve to control our own personal health information and we do not deserve to be punished for our choices or for heath histories which might leave something to be desired. We beg of you, PLEASE PROTECT OUR PRIVACY!!!

Sincerely,

DAWN WINKLER
Vice President

OLSSON, FRANK, AND WEEDA, P.C.
Attorneys at Law
August 3, 1999

The Honorable Bill Thomas
Chairman, Committee on Ways and Means
Subcommittee on Health
United States House of Representatives
Washington, DC. 20515

Dear Chairman Thomas:

I am writing to clarify the record of your Subcommittee's July 20, 1999 hearing regarding confidentiality of health information. At the end of the July 20 hearing, a Member of the Subcommittee asked a question the premise of which was that last year Washington area drug stores sold protected health information to a competing pharmaceutical firm. The premise of this question was apparently based on inaccurate press reports that were later retracted.

In a February 15, 1998, front-page story and February 18, 1998 editorial, the *Washington Post* asserted that Elensys used patient prescription information it received from CVS and Giant for marketing purposes and implied that Elensys sold

patient prescription information to pharmaceutical manufacturers. That is wrong. Elensys does not use prescription information for marketing purposes and has never sold, given, or provided in any way, private pharmacy customer information to any third party.

Elensys is a small business with 20 employees based out of Woburn, Massachusetts. Elensys supports pharmacies in implementing important prescription compliance, therapy management, and education programs. By contract, all of the services Elensys performs are on behalf of and at the direction of the pharmacy. Elensys' contracts with pharmacies expressly prohibit Elensys from utilizing confidential prescription data for its own internal purposes or sharing the information with anyone outside the scope of the agency relationship.

Elensys is committed to supporting pharmacists in offering important healthcare services to their customers. Most importantly, Elensys has always protected the privacy of each patient's health information.

Sincerely,

KAREN A. REIS, COUNSEL
Elensys, Inc.

INDEPENDENCE, MO 64055
July 21, 1999

A. L. Singleton, Chief of Staff
Committee on Ways and Means
US House of Representatives
1102 Longworth House Office Bldg
Washington, DC. 20515

Dear Mr. Singleton:

I am interested in protecting patient privacy, preventing discrimination, and controlling my own health information.

Confidentiality of my patient records is very important to me. Thank you for giving me the opportunity to lend my comments to the July 20th hearing on medical confidentiality.

Patients and doctors have a special relationship requiring the divulging of confidential information that sometimes even the best of friends or family members do not share. There must be trust between the doctor and patient to allow for sharing what could be damaging information in order to allow timely and appropriate medical care.

For the integrity of this relationship and the health care system in general it is important that patients have informed voluntary consent prior to the sharing of information. The bills before the House and Senate do not protect this right. Rather they would create a federal law allowing researchers, government agencies, law enforcement, and managed care organizations to enter my medical records without my authorization. They would also limit the right of my state legislators to enact stronger privacy legislation that Congress enacts.

As an American, I am entitled to certain rights, including the right of protection against unlawful search and seizure by others of my personal property. This includes personal information about myself. Also, the Nuremberg Code protects me against becoming an unwilling research subject.

Unconsented access to my medical records will not only violate my Constitutional rights as a citizen, it will leave me vulnerable to employment, insurance, and medical discrimination. I urge you to truly protect my confidentiality by assuring patient consent prior to all medical record access.

Sincerely,

SANDRA K. GREINER

Statement of Health Insurance Association of America

Confidentiality of Health Information

The Health Insurance Association of America (HIAA) appreciates the opportunity to submit a written statement for the record for the hearing on "Courier New" Con-

fidentiality of Health Information "Courier New" held on July 20, 1999 by the Committee on Ways and Means Subcommittee on Health.

HIAA is the nation leading advocate for the private, market-based health care system. Its more than 269 member companies provide health, long-term care, and disability income insurance coverage to more than 115 million Americans, and offer a range of health care financing products, including indemnity health insurance, managed care plans, preferred provider organization services, Medicare Supplemental ("Medigap") Insurance, Medicare Select, and Medicare+Choice.

HIAA member companies have had, and will continue to have, strict standards in place for protecting patient medical records. In addition, HIAA has been a vocal proponent of the need to protect individually identifiable health information through balanced federal legislation that protects personal health information from public disclosure while ensuring that information is available to carry out basis insurance and health plan functions.

Both public and private payers require personal health information in order to administer health care benefits. As noted by the General Accounting Office (GAO), [p]ersonally identifiable information is essential to the Health Care Financing Administration (HCFA) day-to-day administration of the Medicare Program." [1] Of primary importance is the need for public and private payers to use personally identifiable patient information to pay billions of health care claims annually. Other vital activities that require the use of personally identifiable patient information by public and private payers are:

- Determination of eligibility for benefits;
- Determination of risk-adjustment mechanisms;
- Detection and prevention of fraud and abuse; and
- Review appropriateness and quality of care received by beneficiaries.

In its July 20, 1999 testimony, the GAO also noted several problems faced by HCFA when there are non-uniform state laws for confidentiality of health information. First, if HCFA could not receive uniform health information from sources in all states, there could be an adverse affect on internal operations such as rate setting and quality assurance monitoring. Second, barriers to information gathering could affect the ability of government analysts to perform public policy analysis and health services research because of the burden resulting from compliance with various, non-uniform state laws.

Private payers face similar problems when state confidentiality laws are not uniform. The current patchwork of state laws relating to patient confidentiality leaves consumers with fewer protections in some states than in others. Moreover, laws and regulations governing the collection, use, transmission, and disclosure of health information reach to the heart of the insurance transactional process and thus have a major impact on insurers' core business and systems functions. These critical functions increasingly are carried out across state lines by insurance companies and contractors through the use of computerized data transaction systems. Therefore, health information confidentiality is an area of insurance law in which a significant degree of non-uniformity could impede the industry's ability to operate efficiently and meet the demands of its customers. The resources that must be devoted to compliance with differing state laws in this area can be significant. Adding a new layer of federal regulation without preemption of existing state confidentiality laws would only compound the difficulty. As a result, HIAA would support only those pieces of federal legislation that preempted most state laws.

Consumers' concerns over the confidentiality of health information must be addressed. At the same time, however, we must be careful not to adopt overly prescriptive legislation that undermines the ability of the health care industry to provide these same consumers with the high quality, affordable health care services.

Health information is the lifeblood of the health care system. The days of a patient seeing only a single family practitioner have ended. Today, patients obtain care from a diverse group of health care practitioners, such as specialists and allied health care professionals. In this environment, effective care can only be provided through cooperation among practitioners who must share (and often communicate about) a patient's medical information. As our nation has moved increasingly toward a system of integrated care and computerized transactions, the free flow of medical information becomes even more critical. Accurate, readily available health information is vital to determining the best course of treatment for a patient, and that is clearly its central and most important use.

Also critical is the use of such information to help ensure that basic insurance functions are carried out, such as paying claims and preventing fraud and abuse.

---

[1] *MEDICARE: HCFA Needs to Better Protect Beneficiaries Confidential Health Information* (GAO/T-HEH—99–172, July 20, 1999).

Finally, health information is used for many other purposes: to assure health care quality, to help measure health outcomes, and to ensure that patients receive preventive services, to name only a few. Proposed state and federal confidentiality laws generally contain rules affecting health insurers' and health plans' claims administration, enrollment and disenrollment processes, payment and remittance procedures, referrals and authorization certifications, quality improvement and research activities, and other areas. As such, they can have a significant impact on day-to-day business operations. Therefore, it is critical that balanced, responsible federal legislation be enacted that provides strong protections for consumers while not placing undue regulatory burdens on the private health care system.

In May 1999, the HIAA Board of Directors adopted formal policy supporting the enactment of federal confidentiality legislation that contains several important principles:

• Federal standards for confidentiality of patient health information.

As noted above, federal standards ensuring the confidentiality of patient health information are critical to guaranteeing uniform and consistent treatment of such information throughout the country. Congress took important steps in the right direction with HIPAA by requiring standardized electronic transmission of health care information with appropriate security protections. HIAA believes strongly that a uniform standard is the only way to avoid a dual-regulatory environment for medical records. State authority should remain paramount over areas of confidentiality that do not conflict with national uniformity and consistency, such as state reporting requirements for public health and safety dangers.

• Strong and consistent confidentiality protections for all individually identifiable patient health information.

HIAA believes that all sensitive, personal health information should be kept confidential. Certain types of health information or information about illnesses should not be singled out legislatively for stronger protection, or weaker protections.

• Facilitate appropriate use of patient health information and recognize that access to health information is helpful to patients and often critical to providing quality care.

Today, most health care services are delivered through some form of coordinated or organized system of delivery. As health plans, providers, hospitals, purchasers, and others in the health care industry continue to design and enter into innovative health care delivery arrangements, it is important to recognize that appropriate information sharing and use must occur within that system to ensure patients receive appropriate health care. The trend toward the coordinated delivery of care provides greater opportunities to protect confidential patient health information, and to ensure such information is used appropriately to benefit consumers. Such coordinated systems enable improved tracking of an individual's health information to better monitor appropriate access to and uses of such information.

• Do not impede public and private sector efforts to combat health care waste, fraud, and abuse.

Patient medical information is important to anti-fraud activities carried out both by the state and federal governments, and by insurers. A 1999 audit by the HHS Office of the Inspector General found that Medicare made improper payments of over $12 billion in fiscal year 1998 alone, and the General Accounting Office has estimated that health care fraud accounts for up to 10 percent of national health care spending each year.

Insurance information and patient information are the vehicles through which health care fraud is committed. Providers cannot falsify claims and medical equipment suppliers cannot submit inflated bills without access to patient information. At the same time, this information is critical to combating fraud, as investigators must depend heavily upon the use of medical records to document fraud cases. This does not necessarily mean that individually identifiable patient information must be publicly disclosed in order to successfully investigate and prosecute fraud. But it does mean that fraud investigators in both the public and private sectors must continue to have access to such information. Thus, when developing federal legislation for confidentiality of health information, Congress should be mindful that overly prescriptive privacy protections might adversely affect health care fraud enforcement and ultimately be detrimental to consumers.

• Provide fair penalties as a strong deterrent to misuse of individually identifiable health information, rather than imposing process-oriented regulatory requirements.

HIAA believes that strong administrative penalties should be put in place for those who inappropriately use or disclose sensitive, individually identifiable health information. New penalties should not be authorized for administrative mistakes or errors, but only for material violations that lead to demonstrated harm to consumers.

Statement of Sue A. Blevins, President, Institute for Health Freedom

Chairman Thomas and members of the Ways and Means Subcommittee on Health:

Thank you for holding the important hearing on July 20, 1999 to discuss confidentiality of health information. My name is Sue Blevins. I am founder and president of the Institute for Health Freedom (IHF), a nonpartisan, nonprofit research center dedicated to promoting individual freedom to choose health care.

For nearly three years, Congressional leaders have known that they must pass a medical privacy law by August 21, 1999 or the Clinton Administration will be handed the authority to regulate Americans' medical privacy. The Health Insurance Portability and Accountability Act of 1996 mandates that if Congress fails to act by the August 21 deadline, then regulations governing medical privacy must be promulgated by February 2000. The regulations will affect millions of individuals across the nation, including patients, doctors, law enforcement officials, health insurers, researchers, and government agencies.

Current proposals claiming to make medical information as "non-identifiable as possible" are no guarantee for true medical privacy. Can such vague legislation really guarantee that researchers won't be able to trace back patients' personal information—including genetic and cellular information? With efforts to double the current $15 billion federal budget for biomedical research, it is apparent that scientists are going to need more data to complete research projects. But government has no right to allow researchers access to private-paying patients' medical information without first obtaining their consent.

The Clinton Administration recently announced that its National Bioethics Advisory Commission (NBAC) completed a review of the ethical and medical considerations associated with human stem cell research. The Administration reports that it "recognizes that human stem cell technology's potential medical benefits are compelling and worthy of pursuit, so long as the research is conducted according to the highest ethical standards. NIH is putting in place guidelines and an oversight system that will ensure that the cells are obtained in an ethically sound manner."

The Institute for Health Freedom urges Congress, the Clinton Administration, and the NIH to maintain and enforce strong informed consent principles. Research without consent is unethical.

Statement of LPA, Inc.

Mr. Chairman and Members of the Subcommittee:

Thank you for allowing us to present our views to your Subcommittee regarding medical privacy legislation. LPA, Inc., formerly the Labor Policy Association, is a public policy advocacy organization representing senior human resource executives of more than 250 of the largest corporations doing business in the United States. LPA's purpose is to ensure that U.S. employment policy supports the competitive goals of its member companies and their employees. LPA member companies employ more than 12 million employees, or 12 percent of the private sector workforce.

While there are numerous issues in the medical privacy area where we share the concerns of others within the business community, LPA's primary concern deals with the ability of employers to make critical human resource decisions that serve the interests of employees and the public at large. The principle at stake is whether employers, primarily through fitness-for-duty testing and drug testing, may ensure that employees are not only capable of performing the functions of their position but also that, in doing so, they do not pose a threat to themselves, their co-employees, or the public at large. This concern goes well beyond the bottom-line interests of the employer.

Moreover, we urge the Subcommittee not to overlook the substantial protections that already exist under current law to ensure that employers do not abuse this responsibility. First and foremost, almost ten years ago, the Congress enacted sweeping legislation—the Americans With Disabilities Act (ADA)—that establishes substantial protections for employees regarding employment decisions based on their physical and mental capabilities. As part of those protections, the law imposes carefully crafted restrictions on what employers can ask and how they can use medical information about applicants and employees.

Mr. Chairman, we appreciate the work your staff has done to learn about these issues as it drafted your version of medical privacy legislation. We look forward to working with them further to ensure that final legislation allows employers to meet their obligations to employees and others under current labor and employment laws.

The Executive Branch has not been as responsive. In her September 1996 testimony before Congress, Secretary of Health and Human Services Donna Shalala spoke at great length about the need for specific and far-reaching protections for the personal health information of patients. However, the Secretary's testimony gave far less attention to the very legitimate need of employers for health information for the purposes of ensuring a safe and efficient workplace and complying with existing law.

Under legislation previously introduced in the House—H.R. 1057 and S. 573, the "Medical Information Privacy and Security Act," H.R. 1941, the "Health Information Privacy Act," H.R. 2404, the "Personal Medical Information Protection Act of 1999," and H.R. 2470, the "Medical Information Protection and Research Enhancement Act of 1999"—and in the Senate—S. 578, the "Health Care Personal Information and Nondisclosure Act of 1999" and S. 881, the "Medical Information Protection Act of 1999"—the impact on these restrictions would be, at best, unclear. At worst, the careful balance in the ADA between the individual employee's interests and those of his or her co-employees, the employer and the public would be completely undermined. A similar analysis applies to drug testing which, in many instances, employers are required or encouraged to perform by law.

Since these employer activities have never been the focus of the medical privacy debate, we do not believe the supporters of medical privacy legislation would intend to disrupt them. Instead, it is our sense that, in the rush to enact legislation by the August 1999 deadline, the Congress is still gathering information about all the various endeavors that could be affected, and this is an impact that has not been fully considered. Indeed, after raising these concerns with the Senate Committee on Health, Education, Labor and Pensions, the medical privacy legislation currently under consideration by the Committee now protects these employer activities.

Therefore, it is our purpose today to provide you with the necessary information to assist you in crafting legislation that does not pose a threat to the ability of employers to protect their own employees as well as the public at large.

DRUG AND FITNESS FOR DUTY TESTS

Many jobs require certain levels of physical and/or mental competencies. Fitness for duty examinations allow employers to determine whether an individual can perform the essential functions of the job and, if they are not able to because of a disability, whether a reasonable accommodation can be made to enable them to perform those functions.

The Equal Employment Opportunity Commission, in its January 1992 "Technical Assistance Manual on the Employment Provisions (Title I) of the Americans With Disabilities Act," provides several examples of fitness tests, all of which are consistent with the ADA's protections:

- ensuring that "prospective construction crane operators do not have disabilities such as uncontrolled seizures that would pose a significant risk to other workers;"
- testing of workers in certain health care jobs "to ensure they do not have a current contagious disease or infection that would pose a significant risk of transmission to others;" and
- ensuring that an individual considered for a position operating power saws or other dangerous equipment is not someone "disabled by narcolepsy who frequently and unexpectedly loses consciousness."

In addition to fitness for duty tests, many employers implement drug testing of prospective and current employees. Workplace drug testing, as part of a drug-free workplace policy, has proven extremely effective in reducing work-related accidents. In the 1980s, many companies implemented these programs and began experiencing immediate positive results in their health and safety records. Many of these were described in a 1989 study by the Employment Policy Foundation entitled "Winning the War on Drugs: The Role of Workplace Testing":

- Southern Pacific Transportation Co. first implemented its drug testing program in 1984. According to the company, personal injuries per 200,000 employee hours worked dropped from 15.6 in 1983 to 6.5 in 1988. Train accidents attributable to human failure dropped from 911 incidents in 1983 to 96 in 1988.
- Pacific Gas and Electric Co. enjoyed a 25% reduction in accidents and a 40% decrease in serious injuries after it implemented its pre-employment screening program, designed to alert the company to drug-using job applicants.

• Illinois Bell reported saving $459,000 in reduced absences, accidents and medical disability resulting from a rehabilitation program in which drug-using employees were enrolled.

Because of the success of programs like these, testing in some industries is now even required by law, such as the mandatory drug testing programs for commercial drivers required by the Omnibus Transportation Employee Testing Act of 1991. Even where drug testing is not required, it is often encouraged. Thus, the Drug-Free Workplace Act of 1988 requires all federal contractors with contracts of at least $25,000 to certify that they are providing a drug-free workplace, at the risk of contract debarment if they fail to do so. Many contractors are able to provide this certification as a result of their drug testing programs.

APPLICATION OF PENDING LEGISLATION

None of the bills introduced so far in the 106th Congress contain specific provisions dealing with fitness for duty tests or drug testing. However, it seems clear that the broad definitions of "protected health information" (PHI) under the various bills would encompass the data obtained from those tests, since PHI includes all information that relates to the "past, present or future physical or mental health or condition of an individual" that is "created or received by," among others, an employer.

The bills require that employers obtain a separate authorization from an employee before receiving such protected health information. If the employee refuses to provide the authorization, the employer is forbidden from viewing the results of those tests. This is specifically stated in Section 203 of H.R. 1057 and S. 573 which provides that an employer, health plan, health or life insurers, or providers "may not disclose protected health information to any employees or agents who are responsible for making employment, work assignment, or other personnel decisions with respect to the subject of the information without a separate authorization permitting such disclosure." Section 103 of H.R. 1941 provides that employers may not require an authorization of disclosure of protected health information as a condition of providing or paying for health care.

The requirement for an authorization in these instances is, of itself, not problematic, as long as the employer may take appropriate action where the employee or applicant fails to provide the authorization. Thus, if a job applicant takes a mandatory fitness for duty test, but refuses to authorize disclosure of the results to the employer, the employer should be able to refuse to hire the individual on that basis, or else the test is no longer mandatory.

Two of the bills—H.R. 1057 and S. 573—generally require employers to provide written notice to their employees of, among other things: "The right of an individual not to have employment or the receipt of services conditioned upon the execution by the individual of an authorization for disclosure." This is the only place in the bills where this right is mentioned, but if the bills do indeed create such a right and become law, then an employer would violate the law by refusing to hire an individual who failed to authorize the release of the results of a drug or fitness for duty test.

We believe that Congress has no inclination to prevent employer practices designed to protect the health and safety interests of their employees and the public, particularly in view of the history of strong congressional support for drug testing programs. Thus, we strongly urge this Subcommittee to clarify any medical privacy legislation that it considers to ensure that mandatory fitness and drug testing can continue to exist.

RELATIONSHIP OF LEGISLATION TO EXISTING LAWS

A broader unintended problem is the failure to contemplate the interaction with other laws which may not comprehensively regulate disclosure of individual medical information, but where that information is implicated in the compliance with those laws. In particular, the ability of employers to comply with both the Americans with Disabilities Act (ADA) and the Family and Medical Leave Act (FMLA) could be substantially impaired.

Americans with Disabilities Act. Under the Americans with Disabilities Act, employers are already substantially regulated as to when they can require medical exams of, or request medical information from individuals; what they can examine or ask them for; and what employment decisions are permissible once medical information concerning the individual is acquired. An employer is generally prohibited from discriminating against a "qualified individual with a disability," which means

a disabled individual who can perform the "essential functions of the job" with or without a "reasonable accommodation."

The ADA rightfully recognizes that the employer must have access to a certain amount of medical information about employees and prospective employees. Under Section 102 of the ADA, employers have the right to require a medical examination after an offer of employment has been made and prior to the commencement of employment. If, during the medical examination, the doctor discovers a condition that may affect the person's ability to do the job, the employer still must go through the "reasonable accommodation process" to determine whether the individual could do the essential functions of the job with reasonable accommodation. Once the individual has been hired, the employer may not require medical examinations unless they are "job-related and consistent with business necessity."

Meanwhile, the ADA limits the amount of medical information that can be obtained during employment to that information which is job-related and consistent with business necessity. Strict confidentiality requirements apply to the information. During the hiring process, the employer may share medical information only with decision makers with a "need to know" the information. Even an employee's supervisor and manager are not entitled to any medical information beyond what limitations the employee has to do the particular job. Thus, the ADA already protects against any improper use of critical medical data by the employer.

Yet, the data obtained consistent with ADA requirements would clearly constitute protected health information under legislation introduced so far. Thus, even though the employer would have a right to access the data under the ADA, a new authorization requirement would be superimposed and employers could be forbidden from viewing the results of medical exams taken to detect or confirm the existence of a disability that could affect the ability of an employee to do his or her job competently and safely. While H.R. 1941 provides explicitly that it shall not preempt the Americans with Disabilities Act, the disclosure requirements in the bill make compliance with the ADA potentially problematic.

Family and Medical Leave Act. Under the Family and Medical Leave Act (FMLA), employees are guaranteed a right to up to twelve weeks of leave annually for a serious medical condition. Under Section 103 of the FMLA, employees who wish to use FMLA medical leave can be required by their employer to provide a certification issued by a health care provider that discloses, in part:

- the date on which the employee's "serious medical condition" began;
- the probable duration of the condition;
- the "appropriate medical facts within the knowledge of the health care provider" regarding the condition; and
- a statement that the employee is unable to "perform the functions of the position."

Clearly, most or all of the information contained in the medical certification would meet the definition of protected health information under all the proposed bills, and would therefore be covered by the requirements of those bills. Thus, for the employer to receive the certification, the employee would have to provide the requisite authorization. Since the employer may, under the FMLA, deny leave for an alleged serious medical condition where no certification is provided, could an employee argue that his or her consent was coerced in this situation and thus not valid? This issue must be clarified in the legislation.

CONCLUSION

In conclusion, we believe it is extremely important that any legislation crafted by your Subcommittee in this area recognize the critical role played by medical information in enabling employers to provide necessary protections to their employees as well as the general public. These protections are provided within a framework of existing laws that were carefully crafted to achieve a balance between the competing interests of the individual employee, his or her co-employees, the employer and the public. A dismantling of this framework, whether intended or not, would be disastrous.

Statement of National Association of Health Underwriters, Arlington, VA

The National Association of Health Underwriters is an association of insurance professionals involved in the sale and service of health insurance, long-term care insurance, and related products, serving the insurance needs of over 100 million

Americans. We have almost 16,000 members around the country. We appreciate this opportunity to present our comments regarding confidentiality of health information.

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA), called for Congress to pass legislation to protect the confidentiality of patient medical records no later than August 1, 1999. Should Congress fail to act, HIPAA requires the Department of Health and Human Services to write regulations by February 2000. While there is general agreement on the need for such legislation, it is clear that absolute confidentiality may be unobtainable, and that a balance must be achieved between a person's reasonable desire and expectation of confidentiality, and a payer's right and duty to know what they are paying for.

Technological advances have vastly improved the ability of providers to track patient care and outcomes, develop disease management programs, and exchange information with other providers to improve patient care. These same advances have enabled payers and providers to exchange information quickly to improve the speed and accuracy of claims payment. These technological advances combined with new medical advances in the treatment, and prevention of disease have changed and improved the way medical care is delivered in the United States. When these changes are combined with a now highly mobile society, it becomes clear that the picture of a person's medical records being stored only in the family physician's locked filing cabinet is a thing of the past.

In spite of these changes, NAHU believes that individuals should have an expectation of confidentiality with respect to their personal health information and records. A patient who is fearful that his or her medical records might be disclosed without authorization to a third party may withhold medical information, give false information, or simply not seek treatment for his or her medical condition, resulting in a lack of proper medical treatment, the wrong treatment or no treatment at all.

NAHU believes that individuals have certain rights with respect to their medical records. Individuals should be able to inspect or copy their medical records, to request an amendment to their medical records, and to have a written copy of any disagreement they have with the content of their medical records be listed as a permanent part of their medical file, if their request for amendment is denied.

Health plans, health care providers, public health agencies, researchers, schools, and others who must collect certain medical information should retain on file an authorization for the release of medical information. This authorization allows disclosure of only the medical information necessary to accomplish the purpose for which it is disclosed.

Some groups have called for specialized confidentiality standards on certain "specially protected" portions of a person's medical records, such as information on genetic testing, mental health history, or HIV status. NAHU is opposed to this separation of records for two reasons. First, this approach focuses attention away from the importance of protecting the entire medical record. It is important to note that different individuals have differing ideas about which parts of their medical records are most sensitive. One person may be most sensitive about the results of a genetic test, while another may be concerned about a record of cosmetic surgery. It is impossible for us to know what each person would choose to keep in a "super secret" file, if they had the choice.

Our second concern relates to the practical aspect of keeping two sets of files. For NAHU's members, for example, copies of applications are retained for individuals as well as employer groups that apply for coverage. On small employer plans, individual employees also complete medical questionnaires. So agents may actually have these records on each of 50 employees for each of the employer groups they service, in addition to those of all of the individuals who apply for coverage. Depending on what Congress decided would be kept in which file, not only would our members have to duplicate each file, but they would have to re-screen each application and block out information which could not be retained in the standard file. This merely describes the process for insurance agents, which handle the initial paperwork on an insurance application. Insurance companies would be required to do the same thing. Doctors would have to complete two different medical records, and shift back and forth between both records. All other providers would be required to do the same thing. Not only would the chance for errors in the delivery of medical care increase dramatically, it would greatly increase the cost of delivery of health care. For these reasons, NAHU cannot support a confidentiality proposal that calls for dual record keeping and disclosure requirements.

Thirty-four states currently have some form of confidentiality standards that have been enacted at the state level. Secretary Shalala and some others have suggested that new federal standards should be a "floor," allowing the states to adopt more stringent standards. Many others believe that the interstate way medical care is de-

livered in today's society, the cost implications of fifty separate sets of standards, and the potential confusion for providers and payers, especially those which operate on or near state lines, call for a uniform system nationwide. Confidentiality standards are different from insurance regulations, in that they impact doctors, labs, clinics, hospitals, ambulatory facilities, nursing homes, researchers, and law enforcement officials, in addition to insurance companies, insurance agents, HMOs, and other health plans. In order to truly protect patients, it is important to be absolutely certain that there is no misunderstanding as to the provisions of new confidentiality standards. NAHU believes that a uniform national system would be more easily understood by patients, providers, and payers, and that a single uniform system would be more cost effective. NAHU supports state enforcement authority of these uniform standards.

NAHU has serious concerns about initiatives that would call for a private right of action for breaches of confidentiality. Particularly if state laws are not preempted, the complexities of confidentiality legislation, and the different rules in states that already exist for different types of medical information greatly enhance the opportunity for accidental non-compliance. Legal action is expensive, and the cost will directly affect the cost of health care plans and the premiums people pay for their insurance. If plans become unaffordable, the ranks of the uninsured will increase.

NAHU recognizes that, while medical researchers may generally not require individually identifiable health information, there have been many occasions where it served the public health interest to be able to access individual information, for example, when discoveries have been made relative to dangers associated with certain medications. NAHU believes that researchers subject to peer review should continue to have the opportunity to advise participants in clinical trials or their physicians of these types of negative findings.

Finally, NAHU acknowledges that law enforcement may have a legitimate use for medical records where an authorization for disclosure has not been made, for example, in the lawful interest of public safety when investigating a felony. NAHU believes, however, that these uses should be the exception and not the rule, and that specific requirements for their use should be laid out in legislation, to ensure only appropriate release of information.

NAHU believes that the American consumer will benefit greatly from reasonable and understandable standards for the protection of the confidentiality of medical records. These important protections will make for a healthier America by restoring confidence and trust in the confidentiality of the patient/provider relationship. NAHU looks forward to working with Congress on the passage and implementation of this very important legislation.

We thank you for this opportunity to present testimony to the committee. Should you have any questions, please contact NAHU's Director of Federal Policy Analysis, Janet Trautwein at (703) 276–3806, *jtrautwein@nahu.org*.

Statement of National Association of Insurance Commissioners, Special Committee on Health Insurance

I. INTRODUCTION

This testimony is submitted by the National Association of Insurance Commissioners' (NAIC) (EX) Special Committee on Health Insurance. The NAIC requests that this written testimony be submitted as part of the record for the hearing on "Confidentiality of Health Information" held by the Health Subcommittee of the House Ways and Means Committee.

The NAIC, founded in 1871, is the organization of the chief insurance regulators from the 50 states, the District of Columbia, and four of the U.S. territories. The NAIC's objective is to serve the public by assisting state insurance regulators in fulfilling their regulatory responsibilities. Protection of consumers is the fundamental purpose of insurance regulation.

The NAIC Special Committee on Health Insurance ("Special Committee") is comprised of 46 state insurance regulators. The Special Committee was established as a forum to discuss federal proposals related to health insurance and to provide technical assistance to Congress and the Administration on a nonpartisan basis.

Our testimony focuses on four aspects of the preemption issue raised by the current federal health information privacy legislation. First, we will discuss the states' recognition of the desire for a minimum standard to protect the privacy of health information. Second, we will give some examples of what the states have done to

ensure that health information is kept confidential, and discuss the concerns we have about the preemption language in the proposed federal legislation and how Congress can develop a minimum standard without eliminating existing state protections. Third, we will address the need for Congress to clarify the scope of any federal health information privacy legislation and to develop a way for states to measure their laws against any federal standard for compliance. Finally, we will discuss the enforcement of privacy laws, which may seem to go beyond the issue of preemption, but actually gets to the heart of whether Congress should adopt a floor in this area or completely preempt the states.

II. Recognizing the Desire for a Federal Minimum Standard

As required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress must enact privacy legislation by August 21, 1999. Should Congress fail to act, HIPAA requires the Secretary of Health and Human Services to promulgate regulations by February 2000.

The states, acting through the NAIC, understand the desire for minimum standards to protect the privacy of health information. A minimum standard in this area is considered necessary given that health information is transmitted across state and national boundaries. The transmission of health information, as opposed to the delivery of health care services, is not a local activity. This was one of our main reasons for developing a model on this issue—The Health Information Privacy Model Act (attached).

The NAIC adopted the Health Information Privacy Model Act in September 1998.[1] This model addresses many of the same issues that the federal legislation does, such as: (1) providing an individual the right to access and to amend the individual's protected health information; (2) requiring an entity to obtain an authorization from the individual to collect, use or disclose information; and (3) establishing exceptions to the authorization requirement. Our model was developed to assist the states in drafting uniform standards for ensuring the privacy of health information.[2] However, because our jurisdiction is limited to insurance, and health information privacy encompasses more issues than insurance and more entities than insurers, we understand the desire for broader federal legislation.[3]

Recognizing all of the above factors, along with the fact that all of the health information privacy bills currently before Congress preempt state law in one fashion or another, the members of the NAIC have concluded that the privacy of health in-

---

[1] This model was developed with state regulators, representatives of the insurance and managed care industries, and representatives from the provider and consumer communities. The NAIC model reflects the excellent work that has been done by a number of states on this difficult topic. The NAIC recognized the need to update the provisions of its existing "NAIC Insurance Information and Privacy Protection Model Act," which was adopted by the NAIC in 1980, to reflect the rapidly evolving marketplace for health care and health insurance and the dramatic changes that have occurred over the past 19 years in information technology.

[2] The NAIC model requires carriers to establish procedures for the treatment of all health information, whether or not it is protected health information. The model then establishes additional rules for protected health information. In contrast, the federal bills require that named entities establish and maintain safeguards to protect the confidentiality of *protected* health information, which is more limited. The NAIC believes that Congress should establish procedures to assure the accuracy and integrity of all health information, not just protected health information.

[3] The most obvious difference between the NAIC model and the federal bills is in the scope of the entities to which the respective proposals would apply. The NAIC model applies to *all* insurance carriers. The federal bills are much broader and apply to health care providers, health plans, public health authorities, health oversight agencies, health researchers, *health or life* insurers, employers, schools, universities, law enforcement officials, and agents. Different sections of the federal bills apply to different combinations of these named entities. However, we are concerned that the federal bills only apply to health and life insurers and not to all insurers.

With respect to insurers, we recommend the approach of the NAIC model, which applies to all insurance carriers and is not limited to health and life insurers. The NAIC had an extensive public discussion about whether the NAIC model should apply only to health insurance carriers, or instead, to all carriers. Health and life insurance carriers are not the only types of carriers that use health information to transact their business. Health information is often essential to property and casualty insurers in settling workers' compensation claims and automobile claims involving personal injury, for example. Reinsurers also use protected health information to write reinsurance. The NAIC concluded that it was illogical to apply one set of rules to health insurance carriers but different rules, or no rules, to other carriers that were using the same type of information. Consumers deserve the same protection with respect to their health information, regardless of the entity using it. Nor is it equitable to subject life and health insurance carriers to more stringent rules than those applied to other insurers. Our model applies to all insurance carriers and establishes uniform rules to the greatest extent possible.

formation is one of the few areas where it may be appropriate for the federal government to set a minimum standard. However, it should be noted that up until this point there has been no federal standard in place. Rather, states have been the protector of consumers in this area. Any federal legislation must recognize this fact and make allowances for it.

III. PREEMPTION

A. *Existing State Laws*

As this Subcommittee is well aware, the drafting of legislation to establish standards that protect the privacy rights of individuals with respect to highly personal health information is a very difficult task. Like you, the members of the NAIC sought to write standards into the NAIC Model that would not cripple the flow of useful information, that would not impose prohibitive costs on entities affected by the legislation, and that would not prove impossible to implement in a world that is rapidly changing from paper to electronic records. At the same time, the members of the NAIC recognized the need to assure consumers that their health information is used only for the legitimate purposes for which it was obtained, and that this information is not disclosed without the consumer's consent or knowledge for purposes that may harm or offend the individual.

When developing protections for health information, Congress must recognize the impact of any federal privacy legislation on existing federal and state laws. Although we cannot fully address the impact on federal law, we do know that many state laws touch on protected health information and appear in many locations within the states' statutes and regulations. These laws do not neatly fit into a federal bill's list of exceptions. For example, privacy laws can be found in the insurance code, probate code, and the code of civil procedure. Numerous privacy laws relating to health information are also contained in the states' public health laws, which address such topics as child immunization, laboratory testing, and the licensure of health professionals. Other potential areas involve workers compensation laws, automobile insurance laws, and laws regulating state agencies and institutions. In addition, many state privacy laws only address health programs or health-related information that are unique to a particular state.

Let us give you some examples of the existing state laws that protect health information.

California

California's Business and Professions Code provides protections for health information used in telemedicine, which is the practice of health care delivery, diagnosis, consultation, treatment, transfer of medical data and education using interactive audio, video or data communications (Cal. Bus. & Prof.. Code § 2290.5). These protections are in addition to other existing confidentiality protections provided by law, including the "Confidentiality of Medical Information" statute in California's Civil Code (Cal. Civ. Code § 56 et seq.). Under the telemedicine law, the health care practitioner must obtain verbal and written informed consent from the patient prior to the delivery of health care via telemedicine. The individual retains the option to withhold or withdraw consent at any time without affecting the right to future care or treatment or without risking the loss or withdrawal of any program benefits to which the individual would otherwise be entitled. The patient is guaranteed access to all medical information transmitted during a telemedicine consultation, and copies of this information are available for a reasonable fee. Dissemination of any patient-identifiable images or information from the telemedicine interaction to researchers or other entities is prohibited without the consent of the patient. This statute provides only three exceptions to the requirement of patient consent for disclosure of health information: (1) when a patient is not directly involved in the telemedicine interaction, such as when one health care practitioner consults with another health care practitioner; (2) in an emergency situation in which a patient or representative is unable to give informed consent; and (3) to a patient under the jurisdiction of the Department of Corrections.

California's telemedicine statute could arguably be preempted by federal legislation that uses a total preemption approach. This statute is one example of states responding to changes in technology and addressing issues beyond those addressed in any of the federal bills. California not only protects the confidentiality of medical records but it protects health information in telemedicine. The telemedicine statute also requires consent for disclosing health information and has far fewer exceptions for disclosure without consent than any of the federal bills. The state law also guarantees patients the right to access all medical information without exception, where-

as the federal bills have exceptions to patient access. Finally, the state law allows the patient to revoke consent at any time without affecting the right to future care or program benefits; however, this right is not included in the federal legislation. If a federal privacy bill using a total preemption approach is enacted, California's telemedicine protections, which are stronger than those in the pending federal legislation, would arguably be preempted.

Connecticut

Connecticut has already enacted a privacy protection law for insurance information. (Conn. Gen. Stat. 38a–975 et seq.). This law applies to insurance institutions, agents and insurance-support organizations, and it protects health information that is collected, received or maintained in connection with insurance transactions that pertain to individuals who are residents of the state or who engage in insurance transactions with applicants, individuals or policyholders who are residents of the state. It also applies to insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery, or renewed in the state. This law applies to life, health, disability, and property and casualty insurance, and therefore to issuers of these products. This state law would be preempted under a federal bill that used a total preemption approach. Arguably any health information held by life or health insurers may still be protected under the federal legislation; however, health information held by disability or property and casualty insurers, which is currently protected under this state law, would become unprotected under the current federal legislation. Without the opportunity for the state to implement its own laws to address these types of insurers, the health information they hold would be vulnerable to potential misuse or disclosure by those who hold it. In addition, if the federal standard were to fall short of Connecticut law in some way, the level of protection for information held by life and health insurers would be diminished.

Florida

Florida's Civil Rights law requires confidentiality and informed consent for genetic testing. (Fla. Stat. Ann. § 760.40). The law provides that except for purposes of criminal prosecution, determining paternity, or acquiring specimens from persons convicted of certain offenses, DNA analysis may be performed only with the informed consent of the person to be tested, and the results of such DNA analysis, whether held by a public or private entity, are the exclusive property of the person tested, are confidential, and may not be disclosed without the consent of the person tested. This law arguably would be preempted by a total preemption approach that uses the "related to" standard. Civil rights laws and genetic testing laws do not fall within any of the federal bills' exceptions, so presumably DNA tests would be governed by the provisions of federal bills. However, the federal legislation would arguably allow DNA test results and the identity of the individual to be disclosed without the individual's authorization under some of the federal bills' provisions, including the research provisions.

Massachusetts

Under Massachusetts' education statutes, provisions are established for the testing, treatment and care of persons susceptible to genetically-linked diseases. (Mass. Ann. Laws ch.76, § 15B). The law requires the Department of Public Health to furnish necessary laboratory and testing facilities for a voluntary screening program for sickle cell anemia or for the sickle cell trait and for such genetically-linked diseases as may be determined by the Commissioner of Public Health. Records maintained as part of any screening program must be kept confidential and will not be accessible to anyone other than the Commissioner of Public Health or to the local health department which is conducting the screening program, except by permission of the parents or guardian of any child or adolescent who has been screened. Information on the results of any particular screening program shall be limited to notification of the parent or guardian of the result if the person screened is under the age of 18 or to the person himself if he is over the age of 18. The results may be used otherwise only for collective statistical purposes. Again, this state program may be preempted by a federal privacy law because it does not fall under the federal bills' preemption exceptions. Under the federal bills this health information would be at risk of disclosure without authorization under the public health or research provisions.

Michigan

Michigan's Public Health Code mandates confidentiality of HIV testing and requires written, informed consent (Mich. Comp. Laws. § 333.5114, 333.5133). A physician or the physician's agent shall not order an HIV test for the purpose of diag-

nosing HIV infection without first receiving the written, informed consent of the test subject. Written, informed consent must contain at a minimum all of the following: (1) an explanation of the test, including the purpose of the test, the potential uses and limitations of the test, and the meaning of the test results; (2) an explanation of the rights of the test subject, including the right to withdraw consent prior to the administration of the test, the right to confidentiality of the test and the results, and the right to participate in the test on an anonymous basis; and (3) the persons or class of persons to who the test results may be disclosed. In addition, an individual who undergoes an HIV test at a department-approved testing site may request that the HIV test be performed on an anonymous basis. Staff shall administer the HIV test anonymously and shall obtain consent to the test using a coded system that does not link the individual's identity with the request for the HIV test or the results. The Michigan law states that consent is not required for an HIV test performed for the purpose of research, if the test is performed in such a manner that the identity of the test subject is not revealed to the researcher and the test results are not made known to the test subject. This state law risks being preempted by the federal legislation depending on the preemption approach and the exceptions. If state public health laws are exempt from federal law, this state law could be left in place depending on how the federal legislation classifies public health laws. If state public health laws are not excepted, this state law would arguably be preempted by federal legislation that uses a total preemption approach, but the protection the state law offers would not be replaced with a federal equivalent. Some of the federal bills would allow the identity of the individual to be disclosed without the individual's consent under the public health or research provisions.

Montana

Under Montana's laws governing health maintenance organizations, any data or information pertaining to the diagnosis, treatment, or health of an enrollee or applicant obtained from the enrollee, applicant or a provider by a health maintenance organization must be held in confidence and may not be disclosed to any person, except upon express consent of the enrollee or applicant, pursuant to statute or court order for the production of evidence or discovery, in the event of a claim or litigation between the enrollee or applicant and the health maintenance organization where in the data or information is pertinent, or to the extent necessary to carry out the purposes of this chapter. (Mont. Code Ann. § 33–31–113). The provisions of the state law would presumably be preempted by a total preemption approach and would not be saved under any current exception in the federal bills. The state law prohibits disclosure except in a few limited cases, mostly pertaining to litigation, whereas the federal legislation would allow health maintenance organizations (health plans) to disclose this protected information without authorization under many more instances.

In addition, Montana just enacted a comprehensive medical records privacy bill targeted at insurers. This new law was modeled after the NAIC Health Information Privacy Model Act, and it builds upon Montana's Insurance Information and Privacy Protection Act (Mont. Code Ann. § 33–19–101 et seq.), which is very similar to Connecticut's law (see above). The efforts and careful consideration of the state legislature to adopt privacy legislation would be lost, if the federal privacy legislation preempts all state laws relating to confidentiality of health information.

Ohio

Under Ohio law, information collected by the Ohio Health Care Data Center must be kept confidential, and may only be released in aggregate statistical form. (Ohio Rev. Code Ann. § 3729.46(B)). The Director of Health, employees of the Department of Health including employees of the data center, and any person or governmental entity under contract with the director shall keep confidential any information collected that identifies an individual, including information pertaining to medical history, genetic information, and medical or psychological diagnosis, prognosis, and treatment. Theses persons and entities shall not release such information without the individual's consent, except in summary or statistical form with the prior written permission of the Director or as necessary for the Director to perform his duties. This state law would be preempted by a federal privacy law that totally preempted state law or did not include this type of law as an exception to federal preemption. The state law only allows release of information in summary form without identification of the individual, but this same information risks being released as personally identifiable information under the federal legislation. The federal legislation would end up unprotecting this information that is currently protected under state law.

Vermont

Vermont, like some other states, has a cancer registry. (18 V.S.A. §§ 154, 155, 156). The Vermont statutes require the Vermont Health Commissioner to keep confidential all information reported to the cancer registry, with exceptions for the exchange of confidential information with other states' cancer registries, federal cancer control agencies and health researchers under specified conditions. The provisions of these state laws would arguably be preempted by a federal privacy law that totally preempted state law or did not include state cancer registry laws as an exception to federal preemption. Presumably, a federal privacy law would allow the Vermont Health Commissioner to disclose protected health information in situations not authorized by the state's statutes, but allowed to be disclosed without authorization under the federal bills' public health or research provisions.

These examples should not be construed as a definitive legal analysis of the relationship between these state laws and the federal bills. The comments are not based on an extensive review of all relevant state laws that might affect the ultimate conclusion about the interaction of the federal bills and the states' laws. However, the range of state laws relating to protected health information, and the diversity of their purposes and of the entities that they affect, are critical factors for assessing the impact of any federal preemption language.

B. *The Best Approach to Developing a Federal Standard*

An argument will be made that the only solution to this collection of state privacy laws is a total preemption of state law. However, this "solution" is a deceptively easy response to the various state privacy laws and will most certainly result in adverse, unintended consequences. The language "any State law that relates to matters covered by this Act" could preempt literally hundreds of state laws that affect protected health information.[4] Many state laws that are seemingly unrelated to health information on their face affect health information privacy and could be eliminated by a total preemption approach without any equivalent federal protection. Health information or health-related information that is currently protected will end up unprotected, and states will not be able to remedy the problem or "reprotect" the information. We offer this perspective not to "protect our turf," but rather as a caution against unintended consequences to the consumer. Because of the number and scope of the laws involved, our concerns are not limited to insurance law. We do not want Congress to reduce or eliminate any protections already in place. Preemption of state law is not a workable solution.

We believe the best approach would be to set a federal standard that does not preempt state laws that have been protecting health information for so many years. Up until now, there has been no federal standard in place, and the states have been protecting consumers. We understand the desire to establish a federal floor in this area, but it is not appropriate to preempt stronger state laws or preempt state laws that are outside the scope of the federal privacy legislation. As discussed earlier, the states have enacted privacy protections for their citizens in a variety of areas. These citizens should not lose stronger protections for their health information or lose protections granted by the states in areas not contemplated by the federal legislation.

In addition, we believe that states should be allowed to enact stronger privacy protections in the future in response to innovation in technology and changes in the use of health information. We believe the best approach would balance the desire for uniformity with the recognition of the states' ability to respond quickly and to provide additional protections to their citizens. States can quickly identify the impact of any federal privacy law or any changes in technology or in the use of health information and can efficiently remedy any adverse situation. We urge Congress not to take a "broad-brush" approach to preemption that would unintentionally take away protections at the state level, eliminate the states' ability to remedy unintended consequences that result from federal privacy legislation, or prevent states from responding in the future.

---

[4] This language is very similar to the preemption language contained in the Employee Retirement Income Security Act of 1974 (ERISA), which states: "[T]he provisions of this title...shall supersede any and all State laws insofar as they may now or hereafter relate to any employee benefit plana...." (emphasis added). As this Committee is well aware, twenty-five years of litigation and numerous Supreme Court decisions have yet to clarify the scope of the ERISA preemption language. We would respectfully suggest that a "relate to" standard is not a good standard to adopt in federal legislation regulating the use of health information. Total preemption language will unintentionally erase important state laws but not provide equivalent federal protections. This is the unfortunate situation that has occurred as the result of the preemption language contained in ERISA.

Since Congress is certain to set some type of federal standard, we offer the following language as a suggestion of how federal privacy legislation may be drafted. This language sets a federal minimum standard that leaves in place existing state laws that are at least as protective as the federal legislation and allows states to enact stronger laws in the future.

Nothing in this Act shall be construed as preempting, superseding, or repealing, explicitly or implicitly, any provision of State law or regulation currently in effect or enacted in the future that establishes, implements, or continues in effect any standard or requirement relating to the privacy of protected health information, if such state laws or regulations provide protections for the rights of individuals to the privacy of, and access to, their health information that are at least as protective of the privacy of protected health information as those protections provided for under this Act. Any state laws or regulations governing the privacy of health information or health-related information that are not contemplated by this Act, not addressed by this Act, or which do not directly conflict with this Act, shall not be preempted. Federal law shall not occupy the field of privacy protection. The appropriate federal authority shall promulgate regulations whereby states can measure their laws and regulations against the federal standard.

We believe this language recognizes the desire for a federal standard while respecting what the states have already done.

IV. Scope of the Legislation

In addition to adopting an approach that recognizes the privacy protections already enacted by the states and that allows states the flexibility to enact stronger privacy laws in the future, we urge Congress to draft legislation that specifically outlines the areas that Congress intends to address. Congress needs to be very specific about the scope of any federal privacy legislation. This is of particular concern since the current privacy legislation is silent on many issues affecting federal and state law. The scope should not be left ambiguous or left to the courts to decide. We believe it would be better for the protection of consumers' health information if Congress would specify what is addressed by the federal legislation as opposed to attempting to list all of the state laws that are exempt from the federal legislation.

All of the current federal bills contain specific exceptions to the federal preemption language for certain state laws. Reviewing all of the bills, these exceptions include state laws that: (1) provide for the reporting of vital statistics such as birth or death information; (2) require the reporting of abuse or neglect information about any individual; (3) regulate the disclosure or reporting of information concerning an individual's mental health; (4) relate to public or mental health and prevent or otherwise restrict disclosure of information otherwise permissible under the federal legislation; (5) govern a minor's rights to access protected health information or health care services; (6) relate to the disclosure of protected health information or any other information about a minor to a parent or guardian of such minor; (7) authorize the collecting, analysis, or dissemination of information from an entity for the purpose of developing use, cost effectiveness, performance, or quality data; and (8) concern a privilege of a witness or person in state court.

Although each of the exceptions is appropriate and the list represents a good start at enumerating the specific categories of state laws that should not be preempted, these specific exceptions to the preemption language do not alleviate our concerns. There are other state laws that do not fit into any of the explicit categories and that would therefore be preempted by the broad scope of the general preemption language. In addition, not all of these specified exceptions are included in each of the bills. We mention this to underscore the critical importance of clearly defining the scope of what the federal legislation is addressing and the applicability of any specific privacy standard or exception. We believe it wiser and easier to define what types of health information and what state laws are within the scope of the federal legislation, rather than what types of health information and what state laws are outside of the scope of the federal legislation.

In addition, we urge Congress to outline a way in the federal privacy legislation for the states to measure their laws against any federal standard and to provide options for states to meet those requirements. In HIPAA, Congress gave the states three options in meeting the requirements of that legislation. Similar guidelines are needed in the privacy legislation. States need to be able to judge whether their state laws are stronger than the federal law in order to determine whether they need to take further action to revise their laws.

V. ENFORCEMENT

Finally, we strongly caution Congress against enacting legislation that would preempt state laws, because we have several concerns about the enforcement of any federal privacy law. First, while all of the federal bills include criminal and civil sanctions and some of the bills allow a private right of action, we are concerned about the level of penalties. All of the federal bills include criminal sanctions for those who "knowingly and intentionally" disclose protected health information; however, under such a strict standard, it is unlikely that very many prosecutions will take place at the federal level. The federal bills also impose civil sanctions, but the maximum penalty is only $100,000 for violations occurring so frequently as to be considered a business practice. For a multi-million dollar company, $100,000 can be written off as a business expense. Given the lucrative market for the sale of individually identifiable health information, such an expense could be considered a minor inconvenience.

The states possess a more effective enforcement tool than just monetary penalties. Insurers and other entities, such as hospitals and providers who hold protected health information, are licensed by the state. For repeated violations, the appropriate state agency can revoke the entity's license to do business in the state. This type of penalty forces the entity involved to change its business practices to conform to the law. Total preemption of state law could eliminate this enforcement mechanism.

Second, we also have concerns regarding the federal government's ability to conduct day-to-day oversight and enforcement of these laws. Our internal and informal surveys have shown that states get very few complaints from individuals about inappropriate disclosures of their protected health information. Consumers generally are not aware when a company releases their information. Instead the state agency overseeing that entity uncovers the violation. State insurance departments employ examiners who conduct on-site reviews of insurance companies' files. When a violation is found, it can be corrected immediately. Unless the federal government is prepared to duplicate this system, states should not be preempted from enforcing their own laws.

In addition, state insurance departments offer consumers a place to register their complaints. Those consumers who believe their rights may have been violated can call their state insurance departments and talk with someone about their concerns and have their concerns investigated. We do not believe that this degree of interaction and involvement will exist at the federal level. When a consumer believes his or her rights may have been violated under the new federal law, who in the federal government will that individual call? States already have an enforcement structure in place. This is a structure that should be built upon not preempted.

VI. CONCLUSION

Establishing standards to protect the collection, use, and disclosure of health information is a very important undertaking. The growth of managed care, the increasing use of electronic information, and the advances in medical science and communications technology have dramatically increased both the availability and the importance of health information. The efficient exchange of health information will save thousands of lives. The information is critical for measuring and analyzing the quality and cost effectiveness of the health care provided to consumers. Consumer benefits from advances in health information are vast. However, the potential for misuse of this information is also vast. The information itself has become a valuable product that can be sold for significant amounts of money, and the consequences of unauthorized disclosure of health information can be potentially damaging to individuals' lives. The opportunities to exploit available health information will grow in number and value as technology and medical science advance.

As Members of Congress address this critical topic, we would urge you to recognize the importance of existing state laws addressing the use of health information in many contexts. Congress should be aware of the complexity of implementing federal standards without inadvertently displacing important provisions of state law. We urge Congress not to take a "broad-brush" approach to preemption that would unintentionally take away protections at the state level, eliminate states' ability to remedy unintended consequences that result from federal privacy legislation, or prevent states from responding to future changes in technology or changes in the use of health information. The scope of the preemption is a critical issue, and if not carefully constructed it could lead to unintended consequences. We urge you to recognize the impact of any privacy legislation on federal and state laws as you debate this issue. The members of the NAIC would be happy to work with the Members of Congress in this area. Thank you.

[An attachment is being retained in the Committee files.]

Statement of Margo P. Goldman, MD, and Peter Kane, MSW, LCSW, BCD, National Coalition for Patient Rights, Lexington, MA

Chairman Thomas and members of the Committee. Thank you for the opportunity to submit written testimony on behalf of the National Coalition for Patient Rights (National CPR) about protecting the privacy and confidentiality of health information.

First, we appreciate the Chair's stated commitment to protecting the confidentiality and security of our health information. We agree that these principles are critical to the delivery of quality health care. A patient knowing that his clinician will preserve his privacy and maintain the confidentiality of his medical records is the first pillar to constructing a reliable, efficient, and first-rate health care system. As stated in National CPR's recently published White Paper (included as an attachment), "the primary purpose for collecting personal medical information from a patient is for clinical diagnosis and treatment of that patient. Fundamentally, this is the reason a patient confides information to a physician or other health care provider in the first place." (P2) Such communication frequently occurs when a patient is sick, and therefore, vulnerable. It is done with the expectation originally set forth hundreds of years ago in the Hippocratic Oath—that one's health care provider will not disclose what they have learned about the patient unless the patient agrees for them to do so. This is the basis of trust in the doctor patient relationship.

Unfortunately, patients can no longer trust that their most personal information will remain private. The state of affairs is in critical condition. First, rapidly advancing information technology has created a literal gold mine of medical records. And the feeding frenzy is intensifying. In 1998, CVS and Giant Foods sold prescription data to a Woburn Massachusetts marketing firm in order to promote products. Patients learned of this when they received mail solicitations, specific for their medical conditions. Second, the war against fraud and abuse has led to a virtual assault of patients' privacy. Because HCFA mandated random audits to detect fraud, local Medicare carriers were demanding copies of patient records, including psychotherapy notes, as a condition of processing claims. Finally, as health insurers garner their efforts to contain costs by managing care, more and more sensitive information is demanded and collected. A case in point is the "Erectile Dysfunction Medical Necessity Treatment" form that a local health insurer required from all physicians prescribing medication for impotence. (Copy enclosed) This is but one particularly glaring example where patients are asked to choose between receiving treatments for the most personal of issues and their privacy.

And citizens are reacting to this: A survey recently conducted by the California Healthcare Foundation found 15% of adults said they have done something "out of the ordinary" to keep medical information confidential. This includes self-paying instead of using one's health insurance, avoiding or delaying needed care, giving inaccurate or partial information about medical histories, and asking doctors to not write something down in the record. (California HealthCare Foundation, 1999)

If this trend is allowed to continue, quality health care will be impossible and we will all suffer. Physicians and other health care providers will diagnose and treat patients based on inaccurate or incomplete data. If patients delay or avoid needed care, they will ultimately present for treatment when they are sicker, and less readily (and more expensively) treated. Doctors will increasingly be forced to rely on their memories, rather than the medical record, because of patients' or their own reluctance to record information that may come back to haunt the patient. And sorely necessary biomedical research will be based on tainted data, unless we can ensure that patients trust the system enough to communicate honestly and openly with caregivers.

National CPR was founded over five years ago in response to this grave health care crisis. As an organization whose sole mission has been the patient-centered protection of medical privacy and confidentiality, we have developed policy recommendations. Congress is quickly approaching the August 21 HIPAA deadline to enact legislation; we urge you to use our recommendations (contained in the White Paper) as a basis for sound medical privacy policy. The full White Paper is included as an attachment to our testimony. The recommendations are as follows:

Recommendation 1: Medical records should be maintained as confidential and private for the purpose of the clinical benefits of the patient. Disclosure of medical records outside the context of clinical care requires the consent of the patient.

Recommendation 2: The right of patients to determine what information in their medical records is shared with other providers and other institutions and agencies should be recognized both by law and by institutional policy. Patients who wish not

to disclose medical information to other health care providers that may be important in their medical care should be counseled about the risks of nondisclosure and sign an acknowledgment of their being warned.

Recommendation 3: Patients should have the legal right to review and copy their medical records. Patient access to medical records should be facilitated by providers, and charges to patients limited to the cost of copying. Institutions should develop clear policies and procedures for patients to correct and amend errors in the medical record. Patients should have the right to review the audit trails of who have accessed their medical records and for what purposes.

Recommendation 4: Third party payers of medical services should be required to specify in advance the medical information they require to assess claims and manage medical care. Public notice should be made to patients of the kinds of medical information that will be requested from their providers. Physician notes should not routinely be disclosed to third party payers, and, consistent with the Supreme Court's decision in Jaffe v. Redmond, psychotherapist notes should never be disclosed to third party payers. Patient consent should be required before medical records are transferred to or patients are enrolled in disease management programs. Disease management programs should be based on sound clinical research and arranged through the patient's own health care provider.

Recommendation 5: Third party payers should be held accountable to the same standards of privacy and confidentiality as are medical care providers. Third party payers should be limited in their use of medical records to the terms specified in the patient consent to release medical records. No disclosure by third party payers to any other party may be made without the written freely given consent of the patient, i.e., participation in the health plan or other benefits should not be contingent upon patient consent to further disclosures. Patients of third party medical payers should have the right to review and copy the medical records held by these organizations, and to review the logs of whom has had access to their records and for what purposes. Third party payers should establish procedures for patients to correct errors in their medical information.

Recommendation 6: The psychotherapeutic relationship is of such sensitivity as to require special recognition as a domain of absolute privacy. Records and notes of psychotherapy sessions should always remain confidential and third parties should be prohibited by law from demanding their disclosure for any reason. For reimbursement purposes, only the minimal amount of information should be disclosed to process claims.

Recommendation 7: Research involving medical records must either be conducted with the freely given informed consent of patients, or with blanket consent which delegates to a Medical Records Review Board (MRRB) the authority to waive further consent. The MRRB should be constituted by at least a majority of community members (individuals not employed by or otherwise affiliated with the institution) in addition to appropriate scientific, medical and allied health personnel and administered by the Medical Records Trustee. MRRB decisions not to grant a waiver of informed consent should be final. The MRRB should insure that the confidentiality of patient information is protected as it passes through a research protocol, that the information is not used for other purposes without explicit MRRB approval, and that the purposes of research will not be reasonably objectionable to the patient populations involved.

Recommendation 8: All health services research that relies on personal medical information should be reviewed, approved, and overseen by an institutional Medical Records Review Board, with the Medical Records Trustee being the main point of contact for both patients seeking information about these research/evaluation projects, and for those people conducting the research and/or evaluation projects.

Recommendation 9: Each clinical institution maintaining medical records has the responsibility to safeguard their confidentiality by minimizing access to medical records to those individuals whose "need to know" is of clinical benefit to the patient or is otherwise consented to by the patient. Institutions should employ encryption schemes and password protection, and log each access to or modification of the medical record (e.g., computerized audit trails). Institutions should develop auditing programs to ensure that access to and use of medical records is appropriate and take appropriate punitive measures when it is not. Patients should have the right to limit access to particularly sensitive information.

Recommendation 10: Each health care institution maintaining medical records or medical information should designate a "Medical Records Trustee" responsible for promulgating and enforcing institutional confidentiality and privacy policies, and ensuring compliance with the law. The Medical Records Trustee shall be the final responsible authority for granting any and all access to medical records and information within the institution. The Medical Records Trustee should also be respon-

sible for making notification to patients and the general public of the institution's policies for protecting patient privacy and confidentiality of their medical records.

Recommendation 11: Public health investigations in which an imminent danger to the health of individuals or communities is at stake, should be permitted to access private medical records as necessary and as provided for under current law. The consent of patients is not necessary, but patients should be notified by their providers that their records may be opened to public health authorities. When providers make legally mandated disclosures to public health authorities they should be required to inform the patient of this requirement at the time the condition is discovered.

Recommendation 12: In general, employers should not have access to clinical medical records. These records should be segregated from all other personnel-related information, and be used only in the benefits determination process (and only where the employer is a self-insurer). Employers should be barred from using this information for employment, promotion and other personnel decisions, and provide notification to all employees and prospective employees of what information they collect and for what purposes. Employers with access to medical records should be barred from disclosing this information to other parties, and should maintain audit trails of who has accessed the records and for what purposes, and made available to the employees.

Recommendation 13: Health care institutions maintaining medical records should notify the public and patients individually of the offices and functions which have access to their medical records. Institutions should also prominently display their policies on maintaining confidentiality of medical records. The name, address, and phone number of the Medical Records Trustee should be provided to all patients.

Recommendation 14: Proposals to create systems designed to link private medical information or otherwise collate medical record information, such as the Unique Patient Identifier or the Master Patient Index, should not be implemented without explicit patient informed consent. Patients should always have the freedom to determine for themselves what medical information may be collated together and for what purposes.

Recommendation 15: Law enforcement access to medical records should be limited to court order. When records are thus obtained, they should contain only the minimal amount of information necessary to fulfill the purpose for which they were sought. Moreover, law enforcement officials should maintain the confidentiality of the information they obtain, and should only allow the least number of people access as is absolutely necessary. Under no circumstances should personal medical records become part of an open court record, where the patients are not parties to the court proceeding. In the limited case of health care fraud investigations, anonymous records should be used to assess patterns of fraudulent billing, with identified information used only where specific instances of fraud are suspected.

Recommendation 16: The buying and selling of medical records or information derived from them, and the use of these records for any marketing purposes, including disease management programs, without the freely given informed consent of the patient, should be prohibited by law and institutional policy.

Before we conclude, we will also comment about Federal pre-emption of state and common law privacy protection. As noted in the White paper and elsewhere, a number of states have passed (or are considering) medical privacy legislation that is stronger than some of the Federal proposals. In addition, there exist a host of state common law protections and condition-specific statutes (i.e. HIV, mental health, substance abuse, etc.) to ensure information privacy. The convenience of inter-state information sharing that would be aided by a Federal ceiling of protection does not justify trumping individual and states' rights. Furthermore, "there is no precedent federally for pre-empting state statutory and/or common laws for information-based industries on this sort of scale."(White Paper, p7) National CPR recognizes this is a complicated issue due to the rapidly changing technologies. Because of this, it is critical for states to have legislative flexibility and leeway to search out the best methods of safeguarding their own citizens. Finally, the HIPAA mandate for medical privacy legislation specified that Federal legislation NOT be preemptive. In keeping with Congress' 1996 requirement for Federal law protecting medical information, National CPR strongly urges you to create a Federal floor, not a ceiling, of protection.

Once again, we want to thank Chairman Thomas and the Committee for the opportunity to submit testimony. After over five years of working on medical information privacy, we at National CPR are keenly aware of the complicated nature of the issue and the debate. We gladly offer all possible assistance to the Committee and your staff as you work through this bill.

In conclusion, if Congress fails to enact true, patient-centered medical privacy protection, the quality and integrity of our entire health care system will be in danger. Ann Cavoukian, the Privacy and Information Commissioner in Canada captured this:

"Confidentiality is to medical records, what sterile procedures are to surgery. Having one without the other is not only undesirable, but potentially bad for your health." (May 1996, Ontario, Canada)

[Attachments are being retained in the Committee files.]

NATIONAL CONFERENCE OF
STATE LEGISLATURES
July 19, 1999

The Honorable William M. Thomas
Chairman, Health Subcommittee
Committee on Ways and Means
U.S. House of Representatives
Washington, DC. 20515

The Honorable Fortney Stark
Ranking Member, Health Subcommittee
Committee on Ways and Means
U.S. House of Representatives
Washington, DC. 20515

Dear Representative Thomas and Representative Stark:

On behalf on the National Conference of State Legislatures (NCSL), I would like to take this opportunity to comment on proposals regarding medical records confidentiality.

NCSL firmly believes that states should regulate insurance. We oppose preemption of state law, but we understand the desire to establish a minimum standard in this area given that health information is transmitted across state and national boundaries. We also realize that Congress must enact privacy legislation by August 21, 1999, as set forth by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and we recognize that all of the current approaches set some type of federal standard. Given these factors, we believe that the privacy of health information is one of the few areas where it is appropriate for the federal government to set a minimum standard. Federal medical records confidentiality legislation should provide every American with a basic set or rights regarding their health information. These federal standards, in concert with state law, should be cumulative, providing the maximum protection for our citizens. Our mutual goal should be to assure that not one individual's health information is more vulnerable under federal law, than it was without it.

PREEMPTION OF STATE LAW

Federal legislation should establish basic consumer rights and should only preempt state laws that are less protective than the federal standard. Unfortunately many of the proposals pending before Congress take a different approach.

NCSL is particularly concerned about proposals that would preempt all state laws "relating to" medical records privacy. The universe of state laws relating to medical records confidentiality is extremely large and is spread across a state's legal code. For example, state laws regarding medical records confidentiality can be found in the sections of a state's code regarding: health, mental health, education, juvenile justice, criminal code, civil procedure, family law, labor and employment law.

While no compendium of state confidentiality laws exists, The Health Privacy Project at Georgetown University, part of the Institute for Health Care Research and Policy has just completed a summary of major state statutes related to medical records privacy. It shows that state law in this area is extensive and at a level of detail that is not contemplated in most of the federal proposals. A blanket preemption of state law is virtually the same as throwing the baby out with the bath water.

Should Congress seek to pass federal medical record confidentiality legislation, NCSL firmly believes it should: (1) grandfather existing state confidentiality laws; (2) narrowly and specifically define the scope of the preemption, preserving issues not addressed in the federal proposal for state action; and (3) permit and encourage states to enact legislation that provides additional protections. If states are pre-

cluded in some general way from taking action in specific areas, there must be a mechanism for a state legislature to act if federal legislation adversely impacts the citizens in the state.

Some proposals attempt to address the preemption issue through the inclusion of state legislative "carve outs." This approach attempts to identify all the areas that states would be permitted to continue to enact legislation. While well-intended, there is no way for states to know the full extent and impact of the preemption and carve-outs until the federal law has been implemented. NCSL and the National Association of Insurance Commissioners (NAIC) recommend that states be allowed to continue to legislate and regulate in any area that is not specifically addressed in the federal legislation. Below is language jointly supported by NCSL and NAIC:

Nothing in this Act shall be construed as preempting, superseding, or repealing, explicitly or implicitly, any provision of state law or regulation currently in effect or enacted in the future that establishes, implements, or continues in effect, any standard or requirement relating to the privacy of protected health information., if such laws or regulations provide protections for the rights of individuals to the privacy of, and access to, their health information that are at least as protective of the privacy of protected health information as those protections provided for under this Act. Any state laws or regulations governing the privacy of health information or health-related information that are not contemplated by this Act, shall not be preempted. Federal law shall not occupy the field of privacy protection. The appropriate federal authority shall promulgate regulations whereby states can measure their laws and regulations against the federal standard.

CURRENT STATE LEGISLATIVE ACTIVITY

Since January 1999, 26 states have enacted laws regarding medical records confidentiality. Montana enacted comprehensive legislation addressing the activities of insurers and North Dakota enacted legislation that established comprehensive public health confidentiality standards. After years of debate, Hawaii enacted a comprehensive law that sets standards for the use and disclosure of both public and private health information. Most states enacted legislation building on existing state law or legislation focused on a specific issue. Six laws, addressing a wide variety of medical records privacy concerns, were enacted in Virginia during the 1999 legislative session. Other states that enacted legislation this year are: Arkansas, Colorado, Connecticut, Georgia, Idaho, Indiana, Iowa, Louisiana, Maine, Mississippi, Nebraska, Nevada, New Mexico, Ohio, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, West Virginia and Wyoming.

Several of these new laws address issues that are not addressed in many of the federal proposals. For example, many states have laws establishing strict confidentiality standards for medical information

in the possession of employers. These laws would make records from employee assistance programs (EAP) and workplace drug-testing results, protected health care information, subject to strict disclosure and reporting requirements. Several states have laws that set limits on how much a health care provider can charge an individual to make copies of their medical records. These laws, designed to help assure access, regardless of income, would be preempted under some proposals. These are but a few examples that illustrate both the breadth and complexity of the preemption issue.

I thank you for this opportunity to share the perspective of NCSL on this very important issue. Enclosed for your information is a copy of the NCSL policy, "Principles for Federal Health Insurance Reform." I look forward to working with you and your colleagues over the next several months to develop a consensus proposal that will provide basic medical records privacy protections for all.

Sincerely,

KEMP HANNON
New York Senate
Chair, NCSL Health Committee

cc: Representative Bill Archer
Representative Charles B. Rangel
Members, House Ways and Means Subcommittee on Health

OFFICIAL POLICY

INSURANCE REGULATION

• States should regulate insurance and should continue to set and enforce solvency standards and to provide oversight on insurance matters.
• Modifications to the Employee Retirement Income Security Act of 1974 (ERISA) that would eliminate states' preemption or strengthen the regulatory authority of the states, including consumer access to state remedies, should be adopted. Conversely, NCSL opposes initiatives that would expand the reach of ERISA.
• Absent changes that would permit states to regulate ERISA plans, Congress should impose requirements on ERISA plans that closely track state legislative and regulatory initiatives. In addition, federal remedies, that more closely resemble remedies available at the state level, should be adopted for consumers in ERISA plans.
• Federal legislation that establishes uniform standards, should establish a floor, but not a ceiling.
• When federal insurance reforms are adopted, the consumer should easily understand the implementation process and a massive community education effort should be an integral part of program implementation.
• Federal reforms, that require state enforcement, should be funded by the federal government.
• Any federal legislation requiring state action to comply with the law should allow a reasonable period of time for state legislatures to adequately debate and enact legislation. Where states already have similar legislation in place, a process for declaring "substantial compliance" should be developed.

MEDICAL RECORDS PRIVACY

Scope of Law

• No patient identifiable medical information may be released without written and oral informed consent of the patient, unless otherwise exempted.
• A federal privacy statute should define a range of health care conditions and services and protect patient identifiable information, including demographic information, collected during the health care process.
• A federal privacy statute also should define "information" to include records held in whatever form possible—paper, electronic, or otherwise.
• Strong protections for individuals from the inappropriate disclosure of their medical records should be established.
• Anyone who provides or pays for healthcare or who receives health information from a provider, payer, or an individual should be required to conform to the provisions of the law.
• Health care providers that do not have direct relationships with the patient must also abide by the same standards.
A payer should not be required to provide a benefit or commence or continue payment of a claim in the absence of protected health information, as set forth in each state's statutes, to support or deny the benefit or claim.

Security

• Information should not be used or given out unless either the patient authorizes it or there is a clear legal basis, under state or federal law, for doing so.

Consumer Rights

• Individuals should have the right to:
• Find out what information is in their medical record; and
• How the information is used.
• Practices and procedures must be established that would:
• Require a written explanation from insurers or health care professionals detailing who has access to an individual's information;
• Require insurers or health care professionals to tell individuals how that information is kept;
• Inform individuals how they can restrict or limit access to their medical records;
• Inform individuals how they can authorize disclosures or revoke such authorizations; and
• Inform individuals of their rights should an improper disclosure occur.
• In general, individuals should be permitted to inspect and copy information from their medical record.

• Finally, a process should be developed for patients to seek corrections or amendments to their health information to resolve situations in which coding errors cause patients to be charged for procedures they never receive or to be on record as having conditions or medical histories that are inaccurate.

Accountability

• Severe penalties should be imposed on individuals who knowingly disclose medical records improperly, or who misrepresent themselves to obtain health information.
• Civil monetary and/or criminal penalties should be imposed on individuals who have a demonstrated pattern or practice of unauthorized disclosure.
• Any individual whose rights under the federal privacy law have been violated should be permitted to bring a legal action for actual damages and equitable relief. If the violation was done knowingly, attorney's fees and punitive damages should be available.

Public Health

• Under certain limited circumstances, health care professionals, payers, and those receiving information from them should be permitted to disclose health information without patient authorization to public health authorities for disease reporting, public health investigation, or intervention, as required by state or federal law.

Research

• Research protocols and confidentiality standards should be continued and strengthened.

Law Enforcement

• Law enforcement representatives should be required to have a court order to obtain information from an individual's medical record.

Preemption

• Federal legislation should provide every American with a basic set of rights with respect to health information; however, confidentiality protections provided in state and federal law should be cumulative, and the federal legislation should provide a floor.
• Federal law should only preempt state laws that are less protective.

ADMINISTRATIVE SIMPLIFICATION

• Administrative simplification is a key component in efforts to reduce health care costs and to improve quality of care. Simplification initiatives should include:
• the development of uniform claims forms;
• the establishment and continued refinement of uniform codes;
• electronic claims processing and billing; and
• computerized medical records and "smart cards" for medical records and medical history.
• Federal and state governments should share information; however, confidentiality of medical records and information must be protected.
• Under the provisions of the Health Insurance Portability and Accountability Act of 1996, federal law supercedes state law, except when the Secretary determines that the state law is necessary:
• To prevent fraud and abuse,
• To ensure the appropriate state regulation of insurance or health plans,
• For addressing controlled substances, or for other purposes.

NCSL supports a broad interpretation of this provision that would result in limited preemption of state laws.

July 1998

KANSAS CITY, MO 64111
22 July 1999

A.L. Singleton
Chief of Staff
Committee on Ways and Means
U.S. House of Representatives
1102 Longworth House Office Building
Washington, DC. 20515

Dear Mr. Singleton:

Confidentiality of my patient records is very important to me. Thank you for giving me the opportunity to lend my comments to the July 20th hearing on medical confidentiality.

Patients and doctors have a special relationship requiring the divulging of confidential information that sometimes even the best of friends or family members do not share. There must be trust between the doctor and patient to allow for sharing what could be damaging information in order to allow timely and appropriate medical care.

For the integrity of this relationship and the health care system in general it is important that patients have informed voluntary consent prior to the sharing of information. The bills before the House and Senate do not protect this right. Rather they would create a federal law allowing researchers, government agencies, law enforcement, and managed care organizations to enter my medical records at will. They would also limit the right of my state legislators to enact stronger privacy legislation than Congress enacts.

As an American, I am entitled to certain rights, including the right of protection against unlawful search and seizure by others of my personal property. This includes personal information about myself. Also, the Nuremberg Code protects me against becoming an unwilling research subject.

Unconsented access to my medical records will not only violate my Constitutional rights as a citizen, it will leave me vulnerable to employment, insurance, and medical discrimination. I urge you to truly protect my confidentiality by assuring patient consent prior to all medical record access.

Sincerely,

ELIZABETH S. SMOCK, M.A.

Statement of Randel K. Johnson, Vice President of Labor and Employee Benefits, U.S. Chamber of Commerce

Mr. Chairman and Members of the Committee, good morning. I am Randel Johnson, Vice President, Labor and Employee Benefits, U.S. Chamber of Commerce. The U.S. Chamber of Commerce is the world's largest business federation representing more than three million businesses and organizations of every size, sector and region.

Mr. Chairman, I have been asked to address the narrow issue of whether or not a private cause of action in court should be authorized under the legislation before you today, the "Medical Information and Research Enhancement Act of 1999." We believe the only reasonable answer to this question is "no" and the Chamber would strongly oppose inclusion of a new individual right to sue in addition to the severe civil and criminal penalties already in the legislation. Contrary to the assumptions of some, it is not true that a new right to sue must, or should be, created each time Congress creates a new substantive legal right or that such a right is necessary for effective enforcement. Furthermore, experience would suggest that—given the inherent negatives associated with court litigation—Congress reserve creation of new private causes of action in court for only those situations where there has been a demonstrated and well-documented problem with existing enforcement mechanisms. This threshold criteria has not been met here.

It should be emphasized that whatever is enacted will be an important, but *complicated* new federal law. Before we subject individuals and organizations to the expense and uncertainty of private litigation, we need to allow time for any uncertainties in the law to be clarified. Hopefully, much of this will be accomplished through

administrative regulations that will flesh out the many rights, responsibilities and protections in the legislation, a far preferable course than the vagaries, expense and inconsistencies of the court system developing policy on a case by case basis.

Since the question of whether a private cause of action is necessary turns on whether or not the existing legislation has adequate provisions to deter violations of its provisions, we need to look carefully at what is in the legislation now. I urge the Members to refer to the actual text of the legislation in this regard because these existing sanctions are actually quite severe. First, let's review the criminal penalties under proposed Section 2801 "Wrongful Disclosure of Protected Health Information." Under this section, a "person that knowingly and intentionally"[1] discloses protected health information *shall* be fined up to $50,000, imprisoned not more than one year or both; and if the offense is committed under "false pretenses," be fined not more than $100,000, imprisoned up to five years or both. And if the offense is committed with "the intent to sell, transfer, or use protected health information for monetary gain or malicious harm" the person could be fined up to $250,000, and imprisoned not more than 10 years or both. All of these penalties and prison sentences could be doubled under certain circumstances. I also note that the "person" subject to these sanctions apparently could be anybody employed by, or with any connection to, the health information—from a clerical worker on up; hence the sweep of these provisions is quite broad.

Now let's turn to the civil penalties under new Section 311. Under this section, "a person" who the Secretary of Health and Human Services determines has "substantially and materially failed to comply with this Act" *shall* be subject to up to $500 for each violation and up to $5,000 for multiple violations arising from failure to comply with Title I of the act; and, where a violation relates to Title II, a civil penalty of up to $10,000 for each violation, and up to $50,000 in the aggregate for multiple violations, may be imposed. A $100,000 penalty is provided for violations which constitute a general business practice. This legislation also sets out detailed procedures for consideration of penalties under Section 312. The Secretary is empowered to seek injunctive relief.

To state the obvious, I can assure you that any entity covered by this legislation will take these civil and criminal penalties quite seriously, and I have to ask if there is *anyone* in this room today who would view these possible jail terms and monetary penalties lightly if *they* were subject to this law—I doubt it. I would ask you for one moment to put yourself in the place of an individual within a business handling health care information—of whatever size—and ask yourself that question.

To help demonstrate the extreme nature of these criminal and civil penalties, it might be useful to refer, for the purposes of comparison, to a few employment laws. Under the Occupational Safety and Health Act willful or repeat violations can be penalized by monetary penalties of between $5,000 and $70,000; a serious violation up to $7,000; a non-serious violation up to $7,000, and for failure to correct a violation, a civil penalty of not more than $7,000. With regard to criminal penalties, a willful violation causing an employee's death can be punished by a fine of not more than $10,000 and imprisonment for not more than 6 months or both, except that if the violation is committed after a prior conviction, punishment can be doubled.[2]

The Family and Medical Leave Act and Title VII of the 1964 Civil Rights Act contain no criminal penalties and only a civil fine of $100 for a willful failure to post a notice of FMLA and Title VII rights. The Age Discrimination in Employment Act has a criminal penalty of up to $500 or imprisonment of up to 1 year for interfering with an EEOC agent. Similarly, the National Labor Relations Act, protecting the rights of employees to unionize, provides only for a fine of not more than $5,000 or imprisonment for one year for interfering with a Board agent. The Fair Labor Standards Act contains fines of not more than $10,000 and imprisonment at up to 6 months for certain violations.

As you can see, the proposed civil and criminal penalties of the legislation before you are quite severe in comparison to other laws—laws which also protect important rights.

I led my testimony with a discussion on civil and criminal penalties to dispel any doubt that this legislation somehow provides an invitation for non-compliance or that such penalties are not otherwise adequate to deter violation. *Nothing could be*

---

[1] We urge the committee to define this concept to encompass only knowing and intentional violations of the law in the sense that the individual knew his or her conduct violated the Act and intended harm.

[2] By operation of the 1984 Comprehensive Crime Control and Criminal Fine Collection Act, which standardized penalties and sentences for federal offenses, *willful* violations of the OSH Act resulting in a *loss of human life* are punishable by fines up to $250,000 for individuals and $500,000 for organizations.

further from the truth. In this context, I turn to the question of the need for a private cause of action.

Contrary to what seems to be a popular conception, many laws rely exclusively on government enforcement for protection of important substantive rights, as does this legislation. In the labor area alone these include: The Davis Bacon Act (requires payment of prevailing wages on government contracts for construction), the Service Contract Act (requires payment of prevailing wages on government services contracts), the Walsh-Healey Act (payment of minimum wages and overtime to employees working on government contracts); Executive Order 11246 (prohibits discrimination by government contractors); Section 503 of the Rehabilitation Act (prohibits discrimination by government contractors on the basis of disability), and, perhaps most notably, the Occupational Safety and Health Act (protects employee safety and health), the Mine Safety and Health Act (protects safety and health of miners), and the National Labor Relations Act (protects the rights of employees to engage in concerted activities, including unionization.)[3]

Of course some labor statutes (in interest of full disclosure) do have a private cause of action, typically with remedies keyed to economic damages, such as lost pay with—in some instances—a doubling where the violation was willful or without good faith. (But let me again emphasize that these laws do *not* have the severe criminal and civil penalties contained in the privacy legislation.) An atypical example is Title VII of the 1964 Civil Rights Act, which was amended in 1991 to include non-economic damages (capped at various levels), but only after two years of much contentious debate encompassing two separate Congresses.

These changes were based on a long record of experience amassed over some 30 years, which demonstrated that by the 1990's changes were needed. Even with this lengthy consideration by Congress, the results have not been pretty. Litigation has exploded—tripling since 1991—with discrimination cases constituting almost one of every ten cases in federal court, the second highest number after prisoner petitions.[4] That only 5% of cases filed with the Equal Employment Opportunity Commission are found to have "reasonable cause" and 61% "no reasonable cause," tells us that many of these cases are of questionable validity. I've also attached for the Members' reference an article entitled, "Lawsuits Gone Wild," February 1998, discussing the plight of businesses under this surge of litigation. Litigation expenses alone to defend a case can approach $50,000–$150,000 even before trial.

Perhaps this isn't surprising given the nature of civil litigation, but it does emphasize the importance of Congress carefully deliberating before it authorizes individual civil litigation as a remedy. Indeed, the fact that private lawsuits are expensive, blunt enforcement instruments with enormous transactional costs can hardly be argued. While I do not wish to debate tort reform here, it may be worthwhile to refer to a few further facts on this issue:

A Tillinghast-Towers Perrin analysis (Nov. 1995) of the U.S. tort system found that when viewed as a method of compensating claimants, the U.S. tort system is highly inefficient, returning less than 50 cents on the dollar to the people it is designed to help—and less than 25 cents on the dollar to compensate for actual economic losses. (Tillinghast-Towers Perrin, "Tort Cost Trends: An International Perspective," pp. 4, 8)

The study broke down costs as follows:

Awards for economic loss	24%
Administration	24%
Awards for pain and suffering	22%
Claimants' attorney fees	16%
Defense costs	14%

Hence, even when non-economic "pain and suffering" awards are included, claimants ultimately collected only *46%* of the money raised, the balance going for the high transactional costs of the system.

---

[3] Other examples include the Paperwork Reduction Act, Section 17(a) of the Securities Exchange Act (see Touche Ross v. Redington, 442 U.S. 560 (1979)), and the Federal Service Labor Management Relations Act.

[4] See study by Lawyers Committee on Civil Rights under Law, Daily Labor Report, March 25, 1999. The Americans with Disabilities Act includes the same remedies as Title VII although it was originally passed and enacted with only equitable relief. The ADA was premised on longstanding principles and regulations found under Section 504 of the 1973 Rehabilitation Act. Nevertheless, it, like Title VII since amended by the Civil Rights Act of 1991, has resulted in considerable litigation, much of it frivolous. See "Helping Employers Comply with the ADA," Report of the U.S. Commission on Civil Rights, September 1998, pp. 274–283.

These conclusions are consistent with a 1985 RAND study which indicated that plaintiffs in tort lawsuits in state and federal courts of general jurisdiction received only approximately half of the $29 billion to $36 billion spent in 1985. *The cost of litigation consumed the other half* with about 37% going to attorney's fees (pp. v–xi). A 1988 RAND study of wrongful discharge cases in California found that "total legal fees, including defense billings, sum to over $160,000 per case. The defense and plaintiff lawyer fees represent *more than half* of the money changing hands in this litigation." (pp. viii, 39–40) (The range of jury verdicts were from $7,000 to $8 million with an average of $646,855. pp. vii, 25–27, excluding defense judgements.) (Average award after post-trial settlement and appellate review was still $356,033, p. 36)

A March 1998 study by the Public Policy Institute entitled, "How Lawsuit Lottery is Distorting Justice and Costing New Yorkers Billions of Dollars a Year," applied the Tillinghast-Tower's analysis for New York's tort liability system and calculated that liability expenditures broke out as follows:

- $6.57 billion in payments to claimants (including $3.1 billion in pain and suffering awards and only $3.4 billion for actual economic damages).
- $3.4 billion for *administrative overhead*.
- *$2 billion for defense costs*.
- *And nearly $2.3 billion for plaintiffs' attorneys.*

The study found: "In sum, more than half of the money extracted from our consumers, our taxpayers, and our economy by New York's phenomenally expensive liability system doesn't go to its supposed beneficiaries" (p. 26).

And a May 1995 Hudson Briefing Paper, "The Case for Fundamental Tort Reform" noted that:

- The U.S. tort system needs to be made far more efficient and our society far less litigious and far larger shares of tort payments should go to injured parties rather than to lawyers. Currently, more than fifty cents of every dollar paid out of the tort system goes to cover attorneys' fees.
- Lawyers monopoly of access to the courts allows them to impose a 33.33 to 40 percent toll charge on all damage recoveries, even in cases in which defendants are willing to pay on a rapid no-dispute basis. Contingency fees, the near-uniform means of compensating tort claim attorneys, can provide risk free windfall profits to lawyers while harming defendants, plaintiffs, and the economy as a whole.

The real costs of the nation's tort civil litigation system is enormous[5] , and the broader a civil action is in terms of grounds for liability and damages the more incentive there is for frivolous litigation—as many lawyers and plaintiffs seek to play the litigation lottery in front of juries for huge monetary rewards. However, my primary point here is that simple logic dictates that a system with such heavy transactional costs should, by definition, be considered as an option of last resort.

Of course, I realize that there are those who would argue that a business need not fear litigation so long as it obeys the law—so a provision for civil court litigation should only trouble truly bad actors and not present a problem to others. *The only problem with this argument is that it is patently false.* The reality of laws in this country is that they are invariably complex and, often, simply vague, with the lines of compliance uncertain and often changing. The Code of Federal Regulations governing the workplace arena alone covers over 4,000 pages of fine print, and hundreds of court and administrative decisions provide their own gloss of what the law is, or is not, on any given day. The Supreme Court handed down three decisions on the Americans with Disabilities Act just a month ago and two on what constitutes sexual harassment under Title VII and one on the Age Discrimination in Employment Act in the last session. Eleven Circuit Courts of Appeal render their own versions of the law. One treatise on discrimination law stretches over two volumes and two thousand pages of analysis with more footnotes, as does another on the National Labor Relations Act. And these are not atypical examples of one area of the law. Even enforcement agencies, with all their expertise, cannot give clear answers as to what is or is not required. (See "Workplace Regulation—Information on Selected Employer and Union Practices," GAO Report #94–138)

All of these problems are magnified when it comes to a new law, such as that before you today, which will, no matter how well drafted, be subject to much interpretation. Many times there will not be right or wrong answer and that problem will be heightened if courts across the country, likely combined with jury trials, are imme-

---

[5] For other overviews of expenses associated with court litigation, see, generally, The Illinois Tort Reform Act: Illinois' Landmark Tort Reform: The Sponsor's Explanation, 27 Loy. University of Chicago L. J. 805, Summer 1996. Also see Symposium: Municipal Liability: The Impact of Litigation on Municipalities: Total Cost, Driving Factors, and Cost Containment Mechanisms; 44 Syracuse Law Review 833, 1993.

diately faced with cases to sort out every nuance—which may very well differ from jurisdiction to jurisdiction—while the employer is faced with both uncertain requirements and liability.

In closing, our opposition to inclusion of a private right of action is premised on the straightforward notions that (1) the civil and criminal penalties now in the legislation are quite severe and provide more than adequate deterrence, (2) many laws are adequately enforced without private causes of actions, and (3) law suits are a rough, blunt and expensive instrument of justice with many negative attributes which should only be used where there is a clear track record demonstrating that the law in question currently has inadequate enforcement mechanisms—a record which certainly does not exist here. Should the Congress find that, after passage of this legislation and a period of enforcement, the business community is ignoring its responsibilities, it can always revisit the issue and authorize new enforcement mechanisms.

Thank you.

[Attachments are being retained in Committee files.]