MEDICAL RECORDS CONFIDENTIALITY IN THE MODERN DELIVERY OF HEALTH CARE

HEARING

BEFORE THE

SUBCOMMITTEE ON
HEALTH AND ENVIRONMENT

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

MAY 27, 1999

Serial No. 106–34

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
57–441CC WASHINGTON : 1999

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON HEALTH AND ENVIRONMENT

MICHAEL BILIRAKIS, Florida, *Chairman*

FRED UPTON, Michigan
CLIFF STEARNS, Florida
JAMES C. GREENWOOD, Pennsylvania
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
Vice Chairman
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi
ED BRYANT, Tennessee
TOM BLILEY, Virginia,
(Ex Officio)

SHERROD BROWN, Ohio
HENRY A. WAXMAN, California
FRANK PALLONE, Jr., New Jersey
PETER DEUTSCH, Florida
BART STUPAK, Michigan
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
LOIS CAPPS, California
RALPH M. HALL, Texas
EDOLPHUS TOWNS, New York
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

Page

Testimony of:

Amdur, Robert, Former Associate Professor of Medicine and Chairperson, Dartmouth Committee for the Protection of Human Subjects, Dartmouth Medical School 41

Gencarelli, Dawn M., Manager, Health Policy, Harvard Pilgrim Health Care 54

Hamburg, Margaret A., Assistant Secretary for Planning and Evaluation, Department of Health and Human Services; accompanied by Lana Skirboll, Associate Director for Science Policy, National Institutes of Health; and John Eisenberg, Administrator, Agency for Health Care Policy and Research 10

Jacobsen, Steven J., Director, Section of Clinical Epidemiology, the Mayo Foundation 37

Koyanagi, Chris, Director of Legislative Policy, Judge Bazelon Center for Mental Health Law, on behalf of Consumer Coalition for Health Privacy 92

Krinsky, Daniel L., Director, Patient Services and Pharmacy Practice, Ritzman Pharmacies, Inc 62

Latanich, Terry S., Senior Vice President, Government Affairs, Merck-Medco 68

Meyer, Roberta, Senior Counsel, American Council of Life Insurance 108

Meyers, Abbey, President, National Organization of Rare Disorders 57

O'Keefe, Mark, Commissioner of Insurance, Department of Insurance, State of Montana 100

Stump, David C., Genentech Fellow 44

Visco, Fran, President, National Breast Cancer Coalition 50

Zubeldia, Kepa, Vice President of Technology, Envoy Corporation 84

Material submitted for the record by:

Hamburg, Margaret A., Assistant Secretary for Planning and Evaluation, Department of Health and Human Services, letter enclosing response for the record 120

MEDICAL RECORDS CONFIDENTIALITY IN THE MODERN DELIVERY OF HEALTH CARE

THURSDAY, MAY 27, 1999

HOUSE OF REPRESENTATIVES,
COMMITTEE ON COMMERCE,
SUBCOMMITTEE ON HEALTH AND ENVIRONMENT,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2322, Rayburn House Office Building, Hon. Michael Bilirakis (chairman) presiding.

Members present: Representatives Bilirakis, Deal, Burr, Whitfield, Bryant, Brown, Waxman, Towns, and Eshoo.

Also present: Representative Markey.

Staff present: Marc Wheat, majority counsel; John Manthei, majority counsel; Patrick Morrisey, majority counsel; Karen Folk, minority professional staff; and Amy Droskoski, minority professional staff.

Mr. BILIRAKIS. The hearing will come to order. Good morning. I would like to thank all of you, particularly our witnesses, for gathering today to begin this subcommittee's examination of medical record confidentiality.

The purpose of today's hearing is to have an open discussion, without focusing on any specific legislative proposal, about several contentious issues raised in this debate. I was proud to work on the Health Insurance Portability and Accountability Act of 1996 which allowed portability and removed preexisting restrictions on insurance. Under the act, Congress is mandated to pass legislation addressing the confidentiality of identifiable health information by August 21, 1999. Failure to do so would trigger a requirement that the Secretary of Health and Human Services promulgate regulations by February 1, 2000, to address the confidentiality of administrative data stored and transmitted electronically.

It is significant to note that the Secretary's regulatory authority is more narrow than the broader debate on patient confidentiality. The Secretary's regulations may encompass standards relating to patient health information that is transmitted and stored electronically. However, while the modern health care delivery system is increasingly electronically based, most patient health information remains paper-based.

Medical records contain some of our most sensitive and personal information. There is little argument that patient confidentiality of this information must be safeguarded. Additionally, abuse of this information cannot be tolerated, and everyone must be held accountable for protecting the privacy of this information.

Yet, we must realize the unintended consequences that such legislation may bring about. If legislation goes too far, the quality of health care in this country may be seriously jeopardized. The modern delivery of health care in this country is an integrated system that in many instances no longer involves just patients and their doctors. The system, as we know, has innumerable benefits: disease management programs, protection against adverse drug reactions, and controlling the rising costs of health to ensure that more Americans have access to care.

Additionally, we must make sure that in addressing this problem, we do not unnecessarily compromise ongoing research relating to drugs, medical devices and treatment regimens of approved products. We cannot leave large gaps in our knowledge about products already on the market and prevent new and innovative products from ever being developed. As the subcommittee moves forward, it is my hope that Congress will develop responsible legislation to establish safeguards protecting confidential medical information, encourage strict accountability in how this information may be used, and require tough penalties for misuse of this information.

I would like to welcome our witnesses this morning. I look forward to—and I would like to thank all of you. I look forward to, of course, hearing your testimony. But first I would recognize Mr. Brown for an opening statement.

Mr. BROWN. Thank you, Mr. Chairman.

I would also like to thank the witnesses. In particular, I would like to recognize Dan Krinsky from Ritzman Pharmacies in Wadsworth, Ohio, in my district.

Thank all of you for joining us, Dr. Hamburg, and all of you for joining us today. I am impressed by the scope and the diversity of today's panels. I know that it is sometimes difficult to arrange for a fully representative and balanced list of witnesses, but the value of these subcommittee hearings can hinge on achieving such a balance. I hope that we can continue to work toward that balance for future hearings.

Why is it important to pass a medical records privacy bill? I was struck by a recent piece in The Washington Post about an incident in Alexandria, Virginia. Apparently after a car was stolen near a methadone clinic, the police determined that it would be useful to see the clinical records of all of the patients using the clinic on the premise that this information would somehow help them identify future car thieves.

Without the consent of the patients, they demanded and copied hundreds of private medical records. That doesn't sound like something that should happen in this country, but it happened not too far from the United States capital.

We need to pass a medical records privacy bill. In 1997, Congress assigned itself the responsibility of establishing such protections before August 1999. Several members of this committee, including Mr. Markey and Mr. Waxman, Mr. Towns and Mr. Greenwood have played key roles in enabling Congress to fulfill that commitment. They have done most of the leg work for us.

In light of the complexity of this issue, we owe them a tremendous debt of gratitude for doing that. Now it is our turn to take

a real look at these issues. There is general consensus around the goals, the things that we do and do not want to do. We want to make sure that individuals can gain access to personal medical information; we want to make sure that individuals have the first and last say over personally identifiable medical information, who can see it, who use it, for what purposes.

We also want to encourage participation in medical research by ensuring the confidentiality of any personal information used in that research. What we do not want to do is inappropriately hinder proper and beneficial uses of medical information. The goals may be simple, unfortunately surely striking the right balance between them is not. I am a cosponsor of the Health Information Privacy Act, legislation introduced by Mr. Waxman and Mr. Condit that I believe reconciles these priorities in a way that makes sense and serves the best interests of individuals and the public. But I also think that it is important to keep an open mind as our panelists share their perspectives on two of the most controversial issues addressed in this bill, preemption of State laws and authorization requirements for medical research.

I would also hope in this or a future hearing we could discuss a relevant issue identified by Mr. Towns and addressed in his bill, H.R. 307. That issue involves the fate of medical records when a health care provider or carrier goes out of business. This situation obviously raises access and privacy issues.

The steps this Congress takes in regard to medical records privacy are important to every individual in the United States. Our committee will play a critical role in ensuring a strong effective bill. I look forward, Mr. Chairman, to our future efforts toward that end.

Mr. BILIRAKIS. I thank the gentleman.

Mr. Bryant for an opening statement.

Mr. BRYANT. Thank you, Mr. Chairman.

I will be brief this morning as I know that we have a long list of distinguished witnesses waiting to testify, and I am eager to hear what you have to say.

I will have to excuse myself briefly for a short mark up after my statement, but I do want to return and hear from you so I will be back shortly. When we talk about trying to ensure the confidentiality of the patient identifiable health information in this day and age, the era of technology and Internet and so much information stored electronically, we are talking about no small feat. We can all agree that patient identifiable information should be readily available for patient treatment and securing payment for that treatment.

But there are ongoing discussions about the appropriate uses of information for other purposes including quality improvement, health research, public health, health oversight and the list goes on. We in Congress are now charged with putting together responsible legislation that sets the parameters of how and when and under what circumstances the patient's information can be used and what the penalties would be for violations.

If Congress doesn't pass legislation prior to August 21 of this year, by law, the Secretary of Health and Human Services could put forth regulations regarding electronic medical data. I know a

representative from HHS is here today this morning to outline what their proposal is, but I also know that it is very important to many of my constituents that Congress take the lead in this area. My constituents feel that Congress could do a better job, and they don't want the HHS regulations.

This meeting is the first step in the right direction and I want to thank the chairman and the ranking member for holding this hearing.

I look forward to your testimony, as I said earlier. And I am grateful to the witnesses for taking time out of their busy schedules to be here today, and I would yield back my time.

Mr. BILIRAKIS. I thank the gentleman.

Ms. Eshoo for an opening statement.

Ms. ESHOO. Thank you, Mr. Chairman, for holding this very important hearing today.

First, I want to salute my colleagues, Mr. Markey and Mr. Waxman and the ranking member of the full committee, Mr. Dingell, for the work that they have done in introducing legislation on the issue of medical records privacy.

I think that it is absolutely incumbent upon this Congress to enact a uniform Federal standard of protection for medical records privacy. Currently there isn't any Federal standard. There is an existing patchwork of State laws that provide erratic protection at best. There was a time when our health care privacy was protected by our family doctors who kept handwritten records and those handwritten records were kept in a big file cabinet. I can close my eyes and picture my doctor's office and the pediatrician who took care of my children. Any time that I had a question and I was in the office with him, he would go to that big file cabinet and pull out a bulging file and say they were healthy from the start and here is what we did for them.

With the advent of managed care, increasing numbers of people are involved in health care treatment, payment, and oversight and given access to our very sensitive material. So today we have to place our trust in entire networks of insurers and health care providers. We can no longer expect that information supplied to our doctors will remain confidential.

The American people expect and are entitled to confidential, fair, and respectful treatment of their private health information. But there is another bookend to this issue, and that is research. Research cannot be hampered. It should not be hampered. And I don't think that the American people want it to be hampered. They understand full well what comes from the research because they are the beneficiaries of it.

So we have to be sure that any legislation that is enacted does not erect unnecessary barriers that would slow or impede medical research. I have—and I have bragged about this because I am very proud of it. I have the largest number of biotech companies in my Congressional District more so than any other place in California or our country or the world.

So I see firsthand the advances in medical treatments and therapies that they have produced. Access to health data is vital to the ability to conduct research. I think that we have to keep that on the front burner just as we seek to protect the confidentiality of the

materials. Research has used health records to develop treatments for childhood leukemia and uncovered the link between DES and reproductive cancers. Access to health data plays a critical role in protecting and advancing public health as well.

Our local public health agencies use health records to identify and prevent outbreaks of infectious disease like the recent E.coli infections. Information is the life blood of research. Without access to health data, patients would be, I think, the real losers.

So while I believe that we must establish a uniform Federal standard to protect the American people against the unauthorized use of private identifiable information, I think that we also have to be mindful of what the effects of the laws will be on medical research and the lives that are saved as the outcome of the research.

So thank you, Mr. Chairman, for holding this hearing. It is a very important one. I thank all of the witnesses that are part of today's hearing, and I am also delighted to see that our hearing room is standing room only.

Thank you, Mr. Chairman.

Mr. BILIRAKIS. I thank the gentlelady.

Mr. Whitfield.

Mr. WHITFIELD. Mr. Chairman, thank you very much.

It is quite odd that we have this kind of crowd considering financial modernization is right down on the first floor and I know that it is packed down there.

Mr. Chairman, this is quite an important subject matter that we are going to discuss this morning as we try to balance the need for patient histories for research and adequate medical care versus the privacy of patients. I have in my hand right here a 23 page questionnaire that is now given to home health care agencies when they submit medical assistance to home bound patients.

This is referred to as the "OASIS document" which I understand now is on hold. But during the question and answer series, I would like to ask a couple of questions about this because it makes you wonder if it is necessary to fill out 23 pages of questionnaires about patients.

So this entire subject is quite appropriate at this time. I look forward to the hearing and yield back the balance of my time.

Mr. BILIRAKIS. I thank the gentleman.

Mr. Waxman for an opening statement.

Mr. WAXMAN. I am very pleased that the subcommittee is focusing today on the important issue of medical records privacy. The testimony will be helpful as we work to address the pressing need for legislation that would protect the privacy of health information.

Currently, there is no comprehensive Federal law that protects the privacy of medical records. Instead there is a patchwork of State laws many of which provide minimal protections. Unfortunately, there have been many incidents of inappropriate use and disclosure of such information. Concern about such privacy invasions has led some individuals to avoid medical testing and to withhold information from their physicians.

Congress should enact legislation that protects the privacy of health information and ensures that individuals have appropriate control over their medical records. At the same time, we must allow appropriate access to health information for important public

health purposes such as health research and respect the work that States are doing to address confidentiality issues.

This week I join with Mr. Condit, Mr. Markey, Mr. Dingell, and Mr. Brown and many of my other colleagues to introduce legislation, the Health Information Privacy Act, that I believe strikes the proper balance regarding these issues. We dealt with many of the thorny issues that we will be discussing at this hearing today, and I think that we have a balanced compromise.

The bill is based on three fundamental principles. First, health information should not be used or disclosed without the authorization or knowledge of the individual except in narrow circumstances where there is an overriding public interest.

Second, individuals should have fundamental rights regarding their health records such as the right to access, copy, and amend their records and the opportunity to seek protection for especially sensitive information.

Third, Federal legislation should provide a floor, not a ceiling, so that States and the Secretary of Health and Human Services can establish additional protections as appropriate. This common sense bill reflects consensus among a number of my colleagues who have long been leaders in the area of health care and privacy. And I believe that colleagues with a wide variety of perspectives can support it.

I look forward to hearing from the witnesses today on the complex issues relating to medical records privacy and to working to advance meaningful legislation on this issue.

I thank you, Mr. Chairman, for holding this hearing.

Mr. BILIRAKIS. I thank the gentleman.

Mr. Deal.

Mr. DEAL. Thank you, Mr. Chairman, I would like to thank you, also, and the panelists for being here today.

Like most Members of the last Congress, I received many communications from my constituents with regard to the numbering system that was being proposed. I think that began an awareness on the part of many people on this issue of privacy, and it is certainly one that I think is a delicate balancing act.

Mr. Whitfield alluded to the information form that was being asked to be filled out by home health care agencies. I had occasion recently with my 92-year-old mother who was receiving home health care to overhear the conversation with the home health care nurse who was asking the questions, and as my mother is hard of hearing, it was not difficult to hear the questioning process.

Quite frankly, the questions were so personal and so intensive in nature that I was surprised my mother did not tell him it was none of their business when they asked a few of those questions. So it is something that I think all of us are concerned with, and I thank all of you for being here.

Thank you, Mr. Chairman, for the hearing.

Mr. BILIRAKIS. Thank you. Mr. Towns.

Mr. TOWNS. Thank you, Mr. Chairman, for holding this hearing. I want to commend you for doing this.

As other committee members have indicated, the issue of the privacy of medical records is one that cannot be ignored. Through the rapid growth of modern technology, health records are now readily

available for commercial use, disclosure to employers, and restrictions on eligibility for health insurance. That is why I am pleased to join my colleagues in cosponsoring the Health Information Privacy Act.

I am very pleased that a provision was included in this legislation which would require the Secretary of HHS to promulgate regulations for the maintenance of health records once a facility closes. Currently, there is no uniform method for disposition of a health record if a facility or health benefit plan ceases to exist. You may ask what does happen to that patient's records? Well, it could be destroyed or it could wind up in the street. We really do not know.

Speaking from personal experience of having my own patient records found in the street after hospital closure, I can tell you that it is a problem that will only worsen with the consolidation and merger of various facilities. In fact, we have just seen a number of health plans that are no longer operating Medicare HMO. Can we, in fact, account for all of those patients' records? I do not think so.

Similar provisions which are offered in a larger bill, H.R. 307, have been pointed out by this committee as well at the Government Reform Committee during the last 5 years. Let us know recognize that there is some serious problems in this. The British example is of health record maintenance where the health records of some British royal family members were recently found in the street by a man walking his dog.

It is my hope that any legislation dealing with medical records privacy would contain a means of handling health records once a health facility shuts down or health benefit plan ceases to do business. If we are concerned about continuity of care, we must find a uniform way of dealing with records. Let me also add that a solo practitioner, that when they would expire, the part of the office and all of that would become part of the estate and the family would sell it. But the way that we are delivering medical care today, nobody is going into those offices.

The question is what happens to those records. These are the things, Mr. Chairman, that we really ought to get to the root of if we are really serious about health care and the continuity of it.

Thank you so much.

Mr. BILIRAKIS. I thank the gentleman. You have brought those points up before. They are horror stories. No question about it.

The opening statements of all members of the subcommittee are made a part of the record without objection.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Thank you, Chairman Bilirakis, for holding this important hearing today. The focus of today's hearing is confidentiality of medical records.

As we all know, H.R. 3103, the Health Insurance Portability and Accountability Act of 1996 (HIPPA) directed that within three and one half years after being signed into law that federal laws or federal regulations must be in place to ensure the confidentiality of medical records and other health information. The deadline imposed is close at hand.

With the advances being made in biomedical research, especially genetic research, legislation to protect the confidentiality of health information becomes even more necessary.

Advances in computer technology and the need for administrative efficiencies have created serious issues concerning the confidentiality of patients' medical records.

We must look at the issues related to our changing health care system on a bipartisan basis, maximizing input from patients, academia, researchers, industry, professional groups, and government experts.

As we proceed with how best to craft legislation to create a federal health privacy law, there are several key areas we should look at. For instance, what are the risks to the ability of scientists to do the cutting edge research needed to cure disease, both from failure to address the potential misuse of information by employers and health insurers, as well as from overly restrictive confidentiality regulations?

What legislative and administrative steps can be reasonably taken to maximize the potential for the success of future research?

Can we create an environment that protects the confidentiality rights of the patient and prohibits overt discrimination without infringing on the critical need for scientific progress against deadly and disfiguring diseases?

As we all know, certain white-collar jobs are becoming globally mobile, as employers use low-cost satellite and fiber-optic communications to link U.S. headquarters to companies offering services continents away.

Privacy advocates fear that insurers, employers, and pharmaceutical companies could gain access overseas to peoples medical records. This concerns me and needs to be addressed by Congress.

We should also look at the rights of patients. One question we need to consider is should patients be allowed to access their own medical records.

In conclusion, after passage of legislation to ensure confidentiality and privacy of medical records, we should then move toward the issue of genetic discrimination.

PREPARED STATEMENT OF HON. TOM BLILEY, CHAIRMAN, COMMITTEE ON COMMERCE

Thank you, Chairman Bilirakis for holding this hearing today on the topic of medical records confidentiality.

Every American wants to know that their medical records remain confidential, and that sensitive information that is identifiable to them is not bought and sold and posted on the Internet. No one deserves to have that happen to them.

Many advocates believe that information management systems, statutory protections at the state level, and common law tort theories do not adequately protect medical records data. Some have proposed that a Federal medical records confidentiality "floor" be enacted, on which states could build higher levels of protection.

Others, who believe that present protections are insufficient, favor a Federal law. This approach may allow for a freer flow of critical information, perhaps for research. A federal approach may even cut regulatory compliance costs for enterprises operating interstate.

On Tuesday of this week the National Breast Cancer Coalition recognized the legislative work of this Committee in the area of breast cancer research and early identification. This is an area that is greatly important to me and my family, and I am very pleased that the Coalition's president, Fran Visco, is here today to testify. What causes me concern as I review some of the legislation introduced in the House, is that research to find the cures for diseases like breast cancer will become much more difficult. As someone whose own family has faced breast cancer, I do not want to see legislation going forward that would impede research.

Many bills are being introduced to address challenges in the area of medical records confidentiality. All well-intentioned. Some that are very sound, others I view as mis-guided. Today this hearing affords Members an opportunity to explore issues that directly impact Americans and the interests we all have in privacy, and the confidentiality of our personal information. I urge all the Subcommittee Members to study these issues with great care. It is here in the Congress, and specifically on this Committee, beginning with this panel chaired by Mr. Bilirakis, that these matters will be considered and acted upon. So, Mike, I commend you for holding this hearing, and I yield back my time.

Thank you, Mr. Chairman, and I look forward to the testimony this morning.

PREPARED STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Today the Health and Environment Subcommittee will address the most personal of health care issues, the right of an individual to have control over his or her medical records. I would like to thank my good friend Chairman Mike Bilirakis, for holding a hearing on this important topic, and I look forward to more hearings on the subject in weeks to come.

I am proud to be a cosponsor of the Health Information Privacy Act with Mr. Waxman, Mr. Condit, Mr. Markey, Mr. Brown of Ohio, Mr. Towns, and Mr. Turner. This bill recognizes the fundamental right of an individual to inspect, copy, and amend his or her medical records. It ensures that these records will not be used or disclosed without an individual's knowledge or consent. The bill establishes a federal floor of privacy protections, leaving States the freedom to enact stronger laws patient protections.

Today's hearing covers but two facets of the medical records confidentiality debate—research and preemption. Everyone agrees that medical research is the foundation of twentieth-century medicine, and everyone also acknowledges that protections for patients who are the subject of research are essential. These two interests are not mutually exclusive. Many research studies involve patients with highly sensitive medical records, such as women with breast cancer or people with genetic disorders. We need to enact strong safeguards to protect the very groups who are. most likely to benefit from such research. All research, whether federally-funded or private, should be subject to a check by an institutional review board or a similar entity. The potential harm from a lack of oversight is too great.

A comprehensive federal privacy law would provide many new protections for personal medical records. However, in passing federal legislation we must not preempt the protections that States have already enacted. For example, some States have implemented laws that guard the privacy of certain types of medical information, such as mental health records. State and local laws that are more protective of an individual's privacy rights must be allowed to stand.

There is another, equally important reason for a federal law not to preempt stronger State and local laws. Congress has been considering federal privacy legislation for two decades. If we pass a law this year, it is unlikely that we will revisit the subject any time in the near future. We must not tie the States' hands by preventing them from responding to privacy issues that arise in years ahead.

While there are many facets to the debate over medical records confidentiality, and these issues are often complex, the need for federal legislation is clear. In an age where unauthorized parties may obtain very personal information about ourselves with the click of a computer mouse, we need to assure the public—and ourselves—that our medical information is kept private and secure.

PREPARED STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MASSACHUSETTS

Thank you, Mr. Chairman for holding this hearing on this critical issue, and thank you for permitting me to take part as I am not a member of this Subcommittee.

As you know, I introduced the first medical privacy bill in the House in early March, H.R. 1057, The Medical Information Privacy and Security Act, and this week I joined with my colleagues Mr. Waxman, Mr. Brown, Mr. Dingell and Mr. Condit in introducing a consensus bill.

The August 21 deadline imposed by the Health Insurance Portability and Accountability Act for Congress to pass medical privacy legislation is looming before us. And now is the time for us to move forward on this issue that is of great concern to so many Americans.

Without question, the rapid advance of the Information Age is revolutionizing the American economy and forcing the evolution of new relationships both good and bad. There is no area of its development that causes more anxiety for ordinary people than the area of privacy. And there is no area of privacy that causes more anxiety for Americans than the privacy of their most personal health information.

Today, we are experiencing the erosion of our medical privacy. With the stroke of a few keys on a computer, or the swipe of the prescription drug card, our most intimate and closely held personal health information is being accumulated and tracked.

This erosion of our privacy threatens the very heart of quality health care—doctor/patient confidentiality. By undermining this sacred relationship, we destroy the *trust* that patients rely on for peace of mind, and doctors depend on for sound judgment.

In an HMO today, anywhere from 80-100 employees may have access to a patient's medical record [according to the Privacy Rights Clearinghouse in San Diego California.] With such unrestricted access to one's personal health information, it's impossible to separate the *health privacy keepers* from the "*just curious*" peepers.

Not to mention what I believe is the greatest threat to your medical privacy—the *information reapers.*

The evolution of technology has provided the ability to compile, store and cross reference personal health information, and the dawning of the Information Age has made your intimate health history a valuable commodity.

Last March, the *Wall Street Journal* wrote about the ultimate *information reaper*—a company that is "seeking the mother lode in health 'data mining'". This company is in the process of acquiring medical data on millions of Americans to sell to any buyer.

Currently there is no federal medical privacy law to constrain the *information reapers* as they delve into large data bases filled with the secrets of millions of individuals. These data bases represent a treasure chest to privacy pirates and every facet of your medical information represents a precious jewel to be mined for commercial gain.

With this unfettered access, patient confidentiality has become a *virtual* myth, and the sale of your secrets a *virtual* reality.

Because of the rapid evolution of technology, we have fallen behind in assuring a right that we have come to expect—the fundamental right to keep our personal health information private.

The time is ripe for Congress to take action on this issue. Now is the time to pass a strong medical privacy law that will provide patients the right they deserve, the right to medical privacy.

Mr. Chairman, I thank you again for convening this morning's hearing. I look forward to working with you and our colleagues on both sides to meet the August 21 deadline and I look forward to hearing the testimony of our witnesses presented here this morning.

Mr. BILIRAKIS. I do want to apologize to the witnesses and to the audience for the late start. Obviously you must know that we had a general vote, one of those very tough votes that we sometimes have here, and that delayed the start.

But I would like to now welcome the first panel consisting of Dr. Peggy Hamburg, Assistant Secretary for Planning and Evaluation, Department of Health and Human Services.

Dr. Hamburg, we appreciate your attendance, appreciate your patience, and obviously your written statement is a part of the record. We appreciate it.

I will give you 10 minutes so you can complement your statement in any way that you wish. You might want to introduce your accompanying persons.

STATEMENTS OF MARGARET A. HAMBURG, ASSISTANT SECRETARY FOR PLANNING AND EVALUATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES; ACCOMPANIED BY LANA SKIRBOLL, ASSOCIATE DIRECTOR FOR SCIENCE POLICY, NATIONAL INSTITUTES OF HEALTH; AND JOHN EISENBERG, ADMINISTRATOR, AGENCY FOR HEALTH CARE POLICY AND RESEARCH

Ms. HAMBURG. Thank you, Mr. Chairman, Congressman Brown, distinguished members of the committee. We appreciate the opportunity to appear before you today to discuss the need for Federal legislation to safeguard the privacy of health information.

With me today are Dr. Lana Skirboll from the Office of Science Policy, National Institutes of Health, and Dr. John Eisenberg, who is the administrator of the Agency for Health Care Policy and Research or what we fondly call AHCPR.

I would like to commend the members of this committee, in particular Representative Waxman, Representative Markey, Representative Dingell, Representative Towns, and Representative Brown for their hard work in developing medical privacy legislation. The most recent bill was just introduced on Tuesday, and we have not had the opportunity to review it in detail. We have noted,

however, that the authors chose to take a new approach to the issue and in doing so have helped provide momentum that will be needed to enact legislation this year.

We are here today to emphasize our 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/or be misused. For example, at one HMO, every clinical employee could tap into patients' computer records and see notes from psychotherapy sessions. In another example, the director of a worksite 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 and others you have already spoken to this morning, underline 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 would 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 getting needed treatment, especially for sensitive concerns like mental illness or seeking genetic testing.

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 "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 record keepers. 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 for 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. The consumer should be given clear explanation of these rights.

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

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

As a major payor for health care, our Department is 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, or to conduct the research to learn that beta blocker therapy resulted in fewer rehospitalizations and improved survival among elderly survivors of acute myocardial infarction. Public health agencies use health records to warn us of outbreaks of emerging infectious diseases. Our efforts to improve quality in our health care system depends critically on our ability to review health information.

HIPAA also requires that if Congress fails to enact comprehensive privacy legislation by August of this year, HHS must implement final regulations by February of 2000, as the chairman noted.

We have assembled a team from all of the relevant Federal agencies to work on these regulations, and it is our intent to have these regulations prepared in time for the statutory deadline.

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 has been working closely with many of your staff, and staff in the Senate, to assist you in achieving that goal. Again, let me reiterate that we want to see legislation and we want to work closely with you to make that happen.

Mr. Chairman, the principles embodied in my recommendation should guide a comprehensive law that will create substantive Federal standards and provide our citizens with real peace of mind and protection. 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 us this opportunity to testify, and we are eager to answer any questions that you may have.

[The prepared statement of Margaret A. Hamburg follows:]

PREPARED STATEMENT OF MARGARET A. HAMBURG, ASSISTANT SECRETARY FOR PLANNING AND EVALUATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. Chairman, Congressman Brown, 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. With me today are, Dr. Lana Skirboll, Associate Director for Science Policy, National Institutes of Health, and Dr. John Eisenberg, Administrator of the Agency for Health Care Policy and Research.

I would like commend the members of this Committee, in particular, Rep. Waxman, Rep. Markey, Rep. Dingell, and Rep. Brown for their hard work in developing medical privacy legislation. The most recent bill was just introduced on Tuesday, and we have not had the opportunity to review it in detail. We have noted however, that the authors chose to take a new approach to the issue and in doing so have helped provide momentum that will be needed to enact legislation this year.

As you may remember, Secretary Shalala first presented her recommendations, required by the Congress under Section 264 of the Heath 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 can no longer rely on the existing patchwork of state laws. The patchwork does not provide Americans the privacy protections they need or expect. The Congress should seize upon this opportunity to create strong federal standards and 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 protections 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.

Mr. BILIRAKIS. Thank you, Doctor.

I would say virtually all of the opening statements from members here on both sides of the aisle emphasized, obviously, the sensitive balancing act that is involved here and certainly emphasized the need to not come up with something that would basically hurt research and new ideas.

Having said that, I understand that the report submitted by the Biotechnology and Industrial Organization dated May 27, 1999, fresh off the press, entitled Confidentiality of Patient Medical Records—this, by the way, I would ask unanimous consent to be made part of the record at this point—has reported and I quote them, referring to two bills, H.R. 1057 and H.R. 1941, "contain provisions that will significantly impede medical research by requiring that all research be monitored by an external entity."

[The information referred to follows:]

STATEMENT OF THE BIOTECHNOLOGY INDUSTRY ORGANIZATION (BIO)

CONFIDENTIALITY OF PATIENT MEDICAL RECORDS

EXECUTIVE SUMMARY

The Biotechnology Industry Organization (BIO) is encouraged that the Subcommittee on Health and the Environment of the House Commerce Committee is holding this hearing and working to develop legislation to protect the confidentiality of patient medical records. Although it is critical to protect patients' confidentiality rights, this legislation must be carefully written to allow the continuation of vital medical research. Specifically, federal legislation must recognize that medical researchers use—and sometimes share information and should not impose undue burdens on these efforts. Federal legislation should create national, uniform confidentiality protections, rather than leaving researchers subject to a patchwork of state laws. Further, legislation should not interfere with existing FDA rules governing ad-

verse event reporting. While it is critical to protect patients, imposing too many restrictions on access to important data will slow research efforts. Federal legislation must facilitate the positive uses of medical information to help ensure that the biotechnology industry will continue to make breakthrough scientific achievements into the next century.

STATEMENT

The Biotechnology Industry Organization (BIO) represents 832 companies, academic institutions and state biotechnology centers engaged in biotechnology research on medicines, diagnostics, agriculture, pollution control and industrial applications. BIO would like to take this opportunity to provide input into the continuing congressional debate on legislation to protect the confidentiality of patient medical records.

BIO is pleased that the Congress is developing federal medical confidentiality legislation. As you know, under existing law, if Congress does not act by August of this year responsibility automatically shifts to the Secretary of the Department of Health and Human Services to prepare regulations regarding the use and disclosure of patient information in electronic transactions. Thus, if Congress does not enact legislation, the rules governing patient confidentiality will be a patchwork comprised of these regulations and a myriad of state laws. This environment could slow important research efforts.

BIO has been a supporter of national legislation to protect the confidentiality of medical information. BIO strongly supports enactment of a law that protects patients' confidentiality, just as we supported barring discrimination on the part of group health plans based on "genetic information". We view it as a moral duty—and good public policy—to reassure the public that the great promise of biotechnology research will not be tarnished by abuses of this technology.

However, the legislation must be carefully written to allow the continuation of vital medical research. This research is essential if we are to realize the promise of developing new treatments and cures for many diseases. Legislation that unreasonably restricts researchers' access to and use of medical information will slow, and could halt, research efforts, thereby creating a barrier to the development of new drugs and biologics.

Thus, Congress must craft legislation that balances protecting patients' confidentiality while encouraging research. We are optimistic that this can be accomplished and want to work with you to develop legislation that achieves this balance.

The legislation must carefully define protected health information.

The public has an interest in protecting the confidentiality of identifiable medical information. Information that can be used to identify an individual raises privacy concerns. Therefore, legislation should define "protected health information" to include individually identifiable information to ensure that patients' confidentiality rights are not breached.

Information that is coded, encrypted, or otherwise made anonymous, however, is not as threatening. Use of this data does not raise privacy concerns and therefore should not be subject to the same strict regulations as identifiable information. In addition, this information is critical for health research. For example, it is often used for outcomes research or in disease management programs. This data can provide valuable assistance to researchers as they monitor patient outcomes or try to determine the appropriate dosages for certain drugs. Therefore, legislative language should include information that is coded, encrypted, or made anonymous in its definition of "nonidentifiable health information."

While most of the pending bills contain such a definition, we are concerned that HR 1941, the Health Information Privacy Act, sponsored by Mr. Condit, Mr. Waxman, and others, does not. Legislation that doesn't precisely define nonidentifiable information is likely to have a chilling effect on research because researchers will fear that by sharing certain information they are violating federal law and will be subject to prosecution.

The legislation should not create new external review boards.

Under current law, patients who participate in clinical trials are protected by FDA regulations and the "common rule". This includes safeguards such as oversight by Institutional Review Boards (IRBs), informed consent requirements, and other protections. In certain situations, the common rule provides for expedited review to ensure a timely response to a research request.

Some medical research, however, falls outside the common rule. Examples include medical record review and certain "preclinical" research. Federal confidentiality legislation should not impose excessive restrictions or layers of bureaucracy on this re-

search. Specifically, new legislation should not create an external review process that will impose overly burdensome requirements. Requiring that all research not governed by the common rule be approved by an external review board or satisfy other external monitoring processes will impede research.

Unfortunately, the two bills pending before this subcommittee, HR 1057, the Medical Information Privacy and Security Act, sponsored by Representative Markey, and HR 1941 contain provisions that will significantly impede medical research by requiring that all research be monitored by an external entity. HR 1057 would require all medical research, including research that is privately funded or does not involve human subjects, to be reviewed by an IRB.

HR 1941 goes even farther. It requires that all research be reviewed by an entity certified by the Secretary. It should be noted that this entity is required under the bill to determine that "the importance of the health research outweighs the intrusion into the privacy of the protected individuals who are the subjects of the protected information" before it approves the use of protected information. This standard is more restrictive than that used by IRBs.

Rather than creating additional layers of oversight, legislation should protect patients by establishing clear rules governing the use of information and penalties for violations of these rules.

Federal legislation should create national, uniform protections.

Federal legislation should create national, uniform confidentiality protections. Clinical trials are multi-state ventures. National standards allow researchers to create informed consent and other procedures that will be legal in all states. If federal legislation allows individual states to impose restrictions on top of these standards, research will be slowed.

Strong national standards will also give the public peace of mind because they will know that their medical information is subject to appropriate protections. This, in turn, will make them more willing to share information with medical researchers.

Unfortunately, neither HR 1057 nor HR 1941 provide such standards. By allowing state laws to remain in force, these bills will foster a patchwork of standards and rules that inhibit research.

We urge Congress to enact preemption language that will supersede all state laws that would inhibit access to information important to research. If broad preemption language is not adopted for the provisions of the entire bill, we urge that preemption language governing medical research be adopted.

The legislation should not interfere with existing FDA rules governing adverse event reporting.

The safety of drugs is monitored by existing FDA rules that require physicians and other providers to report to drug manufacturers instances of adverse events for safety and efficacy surveillance. These programs, which are already regulated by the FDA, are an important source of information about the use and efficacy of certain drugs. It is critical that new confidentiality legislation not contain provisions that will discourage reporting and thereby interfere with these programs.

In our view, once again, HR 1057 and HR 1941 fall short since they do not contain these provisions.

The Secretary's Study.

During this debate, some have argued that the Secretary of the Department of Health and Human Services should evaluate the common rule, with an eye toward protecting the confidentiality of patients' medical information. We would urge you to be cautious about legislatively authorizing such a study.

The Secretary already has the authority to study these issues since the common rule requires IRBs to consider patient confidentiality as one of the risks to be evaluated when considering a research request. If federal confidentiality legislation directs her to review the common rule, it should make clear that she should do so in a manner that weighs all the benefits and risks to the subject of the research including short and long term safety and discomfort, and not just focus on confidentiality. Confidentiality concerns should not outweigh other factors. Moreover, the legislation should make clear that the product of any study be a report to Congress, rather than new regulations. Given the controversial nature of this matter, the issues should receive a full debate prior to the promulgation of new regulations.

Conclusion

As the Congress debates confidentiality legislation, we urge you to remember that the public has a strong interest in the medical achievements of biotechnology. The biotechnology industry is on the cusp of developing promising new drugs and treatments for people with serious diseases.

While it is critical to protect patients' confidentiality rights, imposing too many restrictions on access to important data will slow research efforts. Congress must facilitate the positive uses of medical information to continue the breakthrough scientific achievements into the next century.

BIO encourages you to develop this critical legislation. We appreciate the opportunity to submit this statement for the record and look forward to working with you in this endeavor.

Mr. BILIRAKIS. This is so new I am not sure whether you are even familiar with it. I apologize to Mr. Waxman and others if they haven't had an opportunity to see it. I just think that it is significant as we approach it from a generic standpoint.

Do you have any comments regarding that?

Ms. HAMBURG. Well, I have not seen the document that you refer to. But, of course, we appreciate the concerns that many have with the academic community and the private sector with respect to impediments to ongoing research. We do believe, though, that research can be done responsibly and move forward in a framework that involves various levels of privacy protection, oversight, and monitoring. Certainly the research that is supported by the National Institutes of Health goes forward under the circumstances and goes forward in a way that has supported probably the premier researchers and research accomplishments of any place in the world.

Mr. BILIRAKIS. Do either of you have anything that you would care to add?

Mr. EISENBERG. Let me add one thing. I think the three operative words are all, monitored, and external in what you said, all research would be monitored by an external entity.

We do support the idea that research that is carried out with any funds, not just Federal funds, have accountability to be sure that the data that is used, the personnel information that is used, is maintained in a confidential way.

Second, the word "monitored" implies something that is much more aggressive than is usually the process for the institutional review boards which review the proposal for the research. We are asking that there be accountability in the event that the confidentiality promises are breached. But the standard IRB is not to monitor in a very odious way the research that is carried out by investigators.

Third, the term "external" I think could be misunderstood. Institutional review boards are not external organizations. In fact, one of the very important characteristics is that they are internal, that one member of the IRB needs to be someone from outside the organization, but they are internal organizations which are watch dogs to determine that the research is carried out according to the highest principles of research ethics.

Mr. BILIRAKIS. Did you have anything that you wanted to add?

Ms. SKIRBOLL. Yes. I would add that Federal research, that you are well aware of, much of it is records research, health services research, epidemiology now comes under the common rule. The common rule requires an outside entity, if you will, act separate from the investigator to review research.

Research is looked at for both privacy issues, for confidentiality issues, whether research requires informed consent or not. And this is all done in the context of both protecting the privacy of patients,

particularly protecting the privacy of patients that volunteered to participate in research, and, at the same time, ensuring that research can move forward, important research can move forward.

Mr. BILIRAKIS. Well, as I understand it saying in the same point here, according to the written testimony of the Biotechnology and Industrial Organization, H.R. 1941 would expand the Federal Government's role in private research by requiring that all research, whether funded with private dollars or taxpayer dollars, be reviewed by an entity certified by the Secretary using standards that are more restrictive—"more restrictive," their words—than that used by institutional review boards.

Do you agree or disagree that expanding the scope of the Secretary's power over private research and imposing higher compliance costs will impede scientific research? I know that we all are—my time is up, but I know we are all concerned with the biotechnology industries inputs in this regard. And I don't know to what extent the administration has worked with them in working up your proposed regulations, but it is certainly an area that we all need to work on. Very quickly, my time is up, if you would like to respond.

Ms. HAMBURG. I think that it is very important that these issues get aired and discussed. We appreciate this forum and others for that purpose.

I think that ultimately we feel very deeply that the health of our research enterprise depends on the trust and confidence of those participating in research, that their privacy will be protected and confidential data will be handled appropriately. And that if you are participateing in a research study, you probably are not paying attention to what is the source of that funding and distinguishing between what kinds of protections you get from one circumstance and another.

People basically want to have some fundamental sense of confidence that their very personal and sensitive health information will be handled appropriately. We think there are mechanisms to achieve that in the public and private sector.

Mr. BILIRAKIS. Thank you. We have a couple more panels who will probably continue to explore that.

Mr. Brown.

Mr. BROWN. Thank you, Mr. Chairman. Dr. Hamburg, obviously private companies that conduct research have raised questions about the impact of various privacy bills on their operations. Run through, if you would, how the Secretary's recommendations would affect, could affect private sector health research, say a clinical trial for example.

Ms. HAMBURG. I think that I might turn to my colleague from NIH who has looked at this in more specific detail to give you the best possible answer.

Ms. SKIRBOLL. I think it would be important for us to describe how it works for the Federal sector briefly and then explain what the Secretary has recommended.

First of all, it is important to understand that all federally supported research that comes under the common rule, the 17 agencies that signed on to common rule, are protected using both IRBs and informed consent. Walking through that, a researcher has a pro-

posal, the proposal comes to the IRB chair, the IRB chair determines whether that research requires informed consent or does not and whether it requires expedited review or not.

Let me go first to informed consent. Informed consent is a determination of risk, what is the risk to the patient. With medical records, the risk really has to do with privacy and confidentiality. That is weighed and determined whether informed consent should be required in this study or not. If informed consent is required, the common rule says that you must, in the informed consent document, inform the patient the extent to which their privacy will be protected.

If informed consent is waived, then the particular study is considered not risky to privacy and confidentiality or to the risk of the patient. What do I mean by that? The common rule requires that you look at things that we all agree would be risky with regard to confidentiality. Would it be damaging to our financial status, to our employability? Is it stigmatizing? Does it have an affect on reputation.

It cannot be waived if the research is—a review cannot be waived if IRB—it could not be waived if it meets those criteria and informed consent cannot be waived. Much research, much records research, and I could give you examples of each, are waived and no informed consent is required with regard to the issues of burden associated with such IRB review.

The Secretary's recommendations very simply require this. The Secretary's recommendations suggest that without—as long as you are doing research in which there is no informed consent, it does not address informed consent research, where there is no informed consent, there should be an IRB-like entity, some oversight entity that looks to the extent to which confidentiality and privacy are being protected and whether informed consent should be obtained or not.

Mr. BROWN. Thank you, Mr. Chairman.

Thank you.

Mr. BILIRAKIS. Mr. Bryant.

Mr. BRYANT. Thank you, Mr. Chairman.

Let me ask a question. Again, I apologize for missing much of the testimony so far. We did have a short mark up, and it was short. In terms of law enforcement and investigations that might involve health care fraud and abuse, should a privacy bill require—would a privacy bill that you would recommend allow law enforcement officers to come in and just review health care records in a general search for fraud and abuse without any specific probable cause, or is it your view that they ought to have probable cause and obtain a search warrant before they do that? How would you envision any type of legislation to make that——

Ms. HAMBURG. This is obviously a complex and difficult issue. The Secretary's recommendations recognize that there were existing laws at the State and local level with respect to access by law enforcement agencies for this information and recommended that those be allowed to continue to be enforceable and did not really address, in a more comprehensive way, that issue.

Mr. BRYANT. In that event, would you envision—in the event of some sort of inspection by law enforcement officers, would you envi-

sion a requirement in any type of privacy bill that the patient whose records were reviewed be notified that they were inspected and by whom they were inspected?

Ms. HAMBURG. Again, it is a very complex issue. I am not a lawyer, and I would hesitate to make specific comment on that in that I really am uncertain about the legal framework in which that question would have to be answered.

Obviously we would be happy to work with you on that question and bring the right people and resources to bear.

Mr. BRYANT. From a medical standpoint—I am a lawyer, not a doctor. From a medical standpoint is there a difference between privacy, the word privacy, the term privacy, and confidentiality? You nodded your head. You have to speak now.

Ms. SKIRBOLL. By definition, privacy is the right of an individual to limit access and disclosure. Confidentiality is really considered the tools by which you do that, you accomplish that.

So privacy is your right to limit access and confidentiality is the extent to which it actually is disclosed, the tools that you used to keep it confidential. That is sort of a dictionary definition of it.

Mr. BRYANT. Unless any of you have any other comments to the questions——

Mr. EISENBERG. I will just tread on dangerous territory, too, not being a lawyer. But I do think it is important to distinguish whether or not the legal investigation is one that involves the patient or one that involves the provider.

As we look at this issue, we are trying to distinguish the different ways in which the legal community would need to notify or ask for patient permission when the patient is the subject of the investigation versus when it is actually the person providing the care, the patient is the subject.

Most feel that those ought to be distinguished in a different way.

Mr. BRYANT. Mr. Chairman, I yield back the balance of my time at this point.

Mr. BILIRAKIS. I thank the gentleman.

Ms. Eshoo.

Ms. ESHOO. Thank you, Mr. Chairman.

I want to thank the panelists for an excellent presentation. To Peggy, I don't know if all of the members of our subcommittee know of the extraordinarily distinguished family that you come from. Peggy's father most recently headed up the Carnegie Foundation and her family has done extraordinary work. So we have very distinguished people that have given us very important information.

Currently all 50 States have some form of medical records privacy laws and 34 of the States have comprehensive laws. I know that it is not unusual to have hundreds or even thousands of people enrolled in a clinical trial from dozens of States.

What types of burdens can you tell us about that researchers would face if they have to comply with many different laws; and what affects do you think these burdens would have on research?

Ms. HAMBURG. Again, I think that Dr. Skirboll is probably in the best position to answer your question with respect to what is a difficult issue of the patchwork of laws that govern privacy and confidentiality.

Ms. ESHOO. We are going to have to face this in whatever is drawn up.

Ms. SKIRBOLL. I think I described that there are a number of circumstances with regard to records research—Peggy gave some examples of it and so did John—where informed consent is not required to conduct really important research. It gathers important information that improves all of our health and improves the Nation's health.

It is important so that when you look at what States may put into place. Minnesota has a law right now that requires for informed consent for every study of a record. That is an enormous burden to those investigators. We believe that the system in which an IRB, a local IRB, looks at the issues of risk to the patient, allows research to move forward without informed consent, in every situation look at the risks carefully, that it should be allowed to proceed.

States could put into place, in patchwork circumstances, different regulations that would affect a single clinical trial across many States or that would actually bring a halt to research where such informed consent is not practical. So there is a risk. But there needs to be—the Federal position is that there needs—the administration position is there needs to be a floor certainly in which everybody understands there is a common set of rules.

Ms. ESHOO. I am not so sure that I have drawn from what you have said the effects on research as a result of what we have though.

Ms. SKIRBOLL. The effects of research today? Well, Minnesota is an example where it is one State in which being able to conduct records research is significantly hampered because of the requirement that one always get——

Ms. ESHOO. So it is too stringent?

Ms. SKIRBOLL. Yes.

Mr. EISENBERG. May I add something to that?

I think there are three issues that need to be considered when we look at the State-to-State variation that might exist. One of them is it is understandable why the States might be filling the vacuum now in the absence of Federal legislation and with the uncertainty about whether strong Federal regulation and law will exist.

It is understandable that a State would respond to the concerns of the people in that State for privacy and confidentiality legislation. Second, it has only been recently that there have been experts in this field who have been working with the States to help them to draft this kind of legislation.

For example, there was one set of organizations that issued model legislation, but just in February of this year. I think that as the States start to look at—look at this kind of legislation, they will lean upon national experts. I think we will probably start to see more uniformity across the States even without Federal legislation because of the commonality that does exist among the concerned parties.

Third, it is true that the experience in Minnesota is one that we have learned from, but I want to emphasize that we have learned from.

One of the wonderful things about the States in this country is they are, as they say, a cauldron for experimentation.

Ms. ESHOO. Test kitchen.

Mr. EISENBERG. A test kitchen, yes, exactly.

And I think the people in Minnesota would be the first to say that we have learned from the experience there and that there have been modifications made even in Minnesota already in that State's rules.

So as we look at this, I think that the most compelling argument as we look at the States is we need some Federal legislation that will, at a minimum, give as floor so that the States can look at what the Federal Government has done and decide whether anything else is needed.

Ms. ESHOO. Very helpful. Thank you. Thank you, Mr. Chairman.

Mr. BILIRAKIS. I thank the gentlelady. Mr. Whitfield.

Mr. WHITFIELD. Thank you, Mr. Chairman. You had mentioned the difference in privacy and confidentiality. And privacy, I think all of us would view, is this information necessary to provide me the best quality of health care that is available.

I mentioned in my opening statement the outcome and assessment information set that is now—was actually—I guess it was required and then HIPAA backed off of it or HHS backed away. Could you give me an update on precisely where your agency is on the OASIS questionnaire?

Ms. HAMBURG. Perhaps the best way to do that is to provide you specifically in follow-up to this hearing with that information. HICFA is not present, and as you know they have the lead responsibility.

The concerns that you have raised have been addressed. There was, in fact, I think a hearing on the Senate side earlier this week. Modifications have been made. We are very sensitive to the issues, but I think that the specific questions you are asking could best be addressed in follow-up if that is acceptable to you.

Mr. WHITFIELD. Sure. It is my understanding that the American Civil Liberties Union also expressed some concern about those questions as well; is that correct? Are you aware?

Ms. HAMBURG. I do not know the specific details. I do know that this has obviously been the focus of a great deal of attention.

There have been some modifications made in order to focus really on what needs to be asked in the context of appropriate treatment and assuring quality of care to those receiving home care.

And we would be happy to provide you with detailed information about the status of that.

Mr. WHITFIELD. I appreciate that. I recognize the difficulty in dealing with this whole issue. But as Mr. Deal, Nathan Deal, had mentioned as well, when we go back to the district, these home health care agencies are more vocal on this one issue than almost anything else right now.

I don't think there is any group more committed to providing quality health care to the homebound than they are. They have been quite vocal about it. After I had the opportunity to review some of the questions which relates to finances, plans for conception, laundering, housekeeping, shopping, telephone use, it seems that it does go maybe a little bit farther than it should.

While I know that you are not primarily concerned, you are involved, I suppose, in some of the policies over there. I just wanted to raise that issue because it is vitally important.

Thank you again for attending today, and we look forward to working with you to address this issue.

I yield back to Mr. Waxman.

Mr. WAXMAN. Thank you very much. Mr. Chairman, I want to commend Dr. Hamburg and her colleagues and the Secretary for their leadership in this effort.

It will be very helpful for us to discuss with them these issues as we prepare legislation. Let me go back to this point again that we have been discussing and see if we can get it narrowed down.

Mr. Bilirakis expressed concern about the requirement in our bills that the IRB must determine that the importance of health research outweighs the intrusion into the privacy of protected individuals before approving use of the information.

Do you believe this requirement is burdensome on the review process? I want to note that we are going to hear testimony from the Biotech Industry Organization, BIO, where they express the same concern, they even said that we have standards more restrictive than used by our IRBs. Tell us more about—in the answer to this criticism——

Ms. HAMBURG. I think Dr. Eisenberg wants to take——

Mr. WAXMAN. [continuing] expressing legitimate concern. How do you respond to them?

Mr. EISENBERG. I think the second comment that you made about BIO's position is absolutely accurate. That is that the vast majority of the researchers and the vast majority of research organizations in this country have standards that are even more careful, restrictive, if you want to use that word, than we are proposing and more restrictive than current or even future IRBs would require.

The purpose of the proposal is not to make life harder for these organizations, but to be sure there is uniformity so that every patient who is in every study can be sure that they are protected in the way that the best members of BIO are protecting the people in their studies.

I think that is also the case for universities. In all of the universities with which I have been involved, the universities' institutional review board has not really cared whether the study is federally funded or privately funded. The point is that there are patients whose confidential information is at risk and needs to be preserved. Therefore, the standards hold no matter what the source of funding, no matter what the type of study, if the basic principle is followed, which is that you have got to keep personal health information confidential.

We are not, though, suggesting that the current pattern of the IRB for a clinical trial needs to be replicated exactly for the preservation of personal health information's confidentiality. I think that we would prefer to call it an IRB-like mechanism which means that it is an oversight group who provides assurances to the public that that data is maintained in confidentiality.

We would like to work with organizations like BIO and others in the research field to be sure that if there are parts of this process that are burdensome and not necessary that those are eliminated.

Mr. WAXMAN. Do you use IRB-type organizations or IRBs themselves when there is Federal funding for research to look at this very issue of privacy?

Mr. EISENBERG. As Dr. Skirboll mentioned, the common rule requires that if there is Federal funding that an IRB be used.

Mr. WAXMAN. Have we found a problem with that? Has it been burdensome or difficult for researchers?

Ms. SKIRBOLL. I first want to add that beyond the common rule there is a separate set of regulations that FDA, when people come in for an IND that is quite similar to the common rule in many ways.

We believe research has been able to move forward under the context of both the common rule and FDA regulations.

Mr. WAXMAN. One of the most contentious issues in the health privacy debate is whether Federal legislation should preempt State and local laws that are more protective of an individual's privacy.

Proponents of preemption argue that laws that differ from State to State would make business transactions very difficult while opponents argue that a Federal law that preempted all State and local laws would represent a setback to patients of States that have already passed stronger protections.

One compromise that has been proposed is to grandfather in existing State and local laws that are stronger than the Federal statute while preempting any future State and local laws. It seems to me that one drawback of this approach is that States would not be able to respond to privacy issues that may arise in the future, things that we haven't thought about yet.

Would you comment on this? You indicated States are a place where we have a lot of experimentation. We learn from what the States do.

Should we preempt them and stop them from acting in this area?

Ms. HAMBURG. I will try to be brief because I know time is limited.

Mr. WAXMAN. Time is only limited for my asking the question.

Mr. BILIRAKIS. And he still feels that he is chairman sometimes.

Ms. HAMBURG. Well, I think the answer is reasonably straightforward, which is that we clearly need some sort of national legislation which is comprehensive that will set a clear and appropriate floor. States can then elaborate as needed to suit their particular set of needs and concerns, but we do need some sort of baseline and comprehensive floor.

We need that uniformity as illustrated by some of the discussions that we have had this morning.

Mr. WAXMAN. Thank you. Thank you, Mr. Chairman.

Mr. BILIRAKIS. Thank you Mr. Waxman. Mr. Deal.

Mr. DEAL. I will follow up on Representative Waxman's question, and recognizing that all three of you disavowed being associated with the legal profession, my question is somewhat legal in nature but procedural also.

As I understand the timetable we are facing is under the HIPAA Act of 1996, and unless we legislatively here at the Congressional

level establish these guidelines by statute, the Secretary would have the responsibility of developing the guidelines through rules and regulations.

In order to determine where we are on this issue of preemption, is it your understanding that in the absence of Federal action before August that the rules and regs promulgated by the Secretary would, by the HIPAA Act, be given the force and effect of law?

I assume the answer to that would be yes. But if they are given the force and effect of law by that delegation of authority to the Secretary, do they necessarily preempt State statutes? Is there wording enough in HIPAA to preempt State statutes? Where would that stand?

Ms. HAMBURG. I think the most critical issue to put on the table with respect to the Department moving forward with regulations if the Congress doesn't act is that we would not have the authority to provide the kind of comprehensive privacy legislation that we have been talking about today.

The HIPAA requirements clearly limit the authority of the Department in terms of the types of information and the entities that would be regulated. So that through the HIPAA mechanism, I don't think that we would be able to achieve the kind of comprehensive privacy legislation that we feel is so vitally important to the American people.

Mr. DEAL. So you believe then that there is a need for action here to address the issue in a more comprehensive fashion?

Ms. HAMBURG. I think the President and the Secretary feel very strongly that that is the desirable approach.

Mr. DEAL. Taking it one step further, we commonly pass statutes that preempt States for the provisions of existing State law that are not as comprehensive, but allow them to go further than the Federal standard that is established.

My question is in the earlier discussions about the problems that you were running into from State-to-State variations, it was the State statutes in Minnesota, for example, that went further that were the impediments to the research component.

So if we pass a Federal statute, but still allow States to go further, do we not still leave intact those impediments to research and compilation of information by those who are so restrictive that they are an impediment?

Ms. HAMBURG. I think as Dr. Eisenberg pointed out earlier, one of our concerns is that States are moving because they are trying to fill a vacuum that exists because we don't have a national approach. So it is our hope that if we do achieve a national comprehensive legislative approach that much of what we have seen on the State level will not be necessary.

But our health care system is very complex. How it is—how health care is delivered varies by State to State. Technologies are changing, and it raises different issues and States may react differently. So that if we established uniform and a more comprehensive set of protections at the national level, it would address many of the concerns that States are currently experiencing.

But there would still be flexibility for modifications based on the particular set of needs and concerns that might exist within a State.

Mr. DEAL. One final quick question, if I might. In reviewing the recommendations from the Southern Governors Association and their concerns as we address this issue, one issue they have raised is that consent forms not be so broad as to allow consent for one purpose but be broad enough to allow the sale of information for other purposes.

Are you seeing problems with consent forms being so broad that a person waives rights that perhaps were never intended, and if that is the case, is that an issue we need to focus on in drafting legislation?

Ms. SKIRBOLL. That is an important point. I think it is important to note that most of the legislation that has been drafted so far, most of the considerations that really have been addressed in terms of privacy and confidentiality, have to do with records for which there is no consent without disclosure to the patient.

There hasn't been a lot of consideration if there is consent, what that consent might look at. That is something an IRB does, but most of the legislation has really been addressing disclosure without patient authorization.

Mr. DEAL. Thank you, Mr. Chairman.

Mr. BILIRAKIS. Mr. Burr.

Mr. BURR. Thank you, Mr. Chairman.

Dr. Hamburg, let me go back to Mr. Deal and Mr. Waxman's question.

I read your testimony, and I actually wrote on that testimony that it said you wanted to preempt. But I heard your answer to both questions where both times you stated what we need to do is create a floor and to allow States to go further. And I would only ask you is that inconsistent with what your testimony says, which is the concern of patchwork, a patchwork situation.

And I know that you referred to the patchwork in the context of the privacy protections that Americans need and expect. Is it the floor or is it the preemptive ceiling that HHS would choose?

Ms. HAMBURG. It is clearly our strong desire and preference to have a strong national privacy legislation that would address the set of concerns that American citizens have regardless of where they live.

We recognize also, though, that there are differing issues in different States with respect to constituencies, how health care is delivered, et cetera, and that we need to have a somewhat flexible approach.

But there needs to be a floor in terms of a set of comprehensive national standards.

Mr. BURR. I think what I just heard was a modified preemption. Would that be an accurate depiction of it? A fluid process; let's say?

Ms. HAMBURG. A flexible approach, but I think building on a foundation that represents a set of uniform national standards.

Mr. BURR. Ms. Skirboll—is that it? I am sorry; I came in late.

Let me just ask—NIH has been used in the IRB for archival research and I guess I would ask you, have you ever found incidents of abuse? Has the NIH experienced incidents of abuse?

Ms. SKIRBOLL. Abuse with regard to privacy and confidentialty?

Mr. BURR. Yes, ma'am.

Ms. SKIRBOLL. That is really under the responsibilities of OPRR which is housed in NIH, but really is responsible for the coverage of the common rule which is 17 agencies. You probably have to ask the director of OPRR that. But I think, in general, where there is regulation there certainly can be abuse, but the purpose of this—the purpose of having the common rule and having a local jurisdiction is that there is monitoring by the IRB during the process of research, and that if exigencies happen, they can be found.

Mr. BURR. I would assume if there was this horror story of abuses, that would not be limited in the knowledge of it to just that area of NIH, but it would be known throughout NIH.

Ms. SKIRBOLL. Privacy is an interesting thing with regard to abuse.

Most people, and I take this from the director of OPRR, most people say when there has been a breach of privacy, by definition, people don't want to talk about it because it causes the further breach of whatever private information was breached in the first place.

So perhaps knowledge—breaches of privacy are not known as widely as information of other problems that may arise. So we really haven't tracked that.

Mr. BURR. I am also not a lawyer, never professed to ever want to be, have discomfort sitting next to one, but Dr. Hamburg, let me ask you more of a legal question and it comes from your testimony.

You said information should not be used or given out unless either the patient authorizes it or there is a clear legal basis for doing so. Can you give me an example of a clear legal basis?

Ms. HAMBURG. Well, for example, before I joined the department, I was commissioner of health in New York City and responsible for the public health and safety of New Yorkers.

In order to respond to unusual clusters of disease and apparent outbreaks of an infectious disease, we often needed to access information with identifiers so that we could do a complete and appropriate outbreak investigation, identify the source of whatever infectious agent or contaminant was threatening the health of the public and ameliorate that threat by instituting the appropriate measures.

And we had the legal authority to do that, and it was extremely important to public health and safety.

Mr. BURR. But HHS would not see defining what a clear legal authority would be?

Ms. HAMBURG. Well, I think——

Mr. BURR. Every time I see "clear legal authority," I think that we have—we have punted to the judicial system which is not necessarily a comfort for everybody involved to think that either HHS would promulgate some new regs or the Congress would pass new legislation, only for the courts to try to figure out how to share with everybody what we meant.

Mr. BILIRAKIS. The gentleman's time has expired. If you have a quick response to that, please feel free.

Ms. HAMBURG. I think it is very important that we define the set of circumstances under which health information could be disclosed without authorization.

The example I gave of public health was one that was identified within the secretary's recommendations. Clearly we live in a very complicated and changing world. And I think that we could not produce legislation that would clearly identify and define all of the specifics, but I think that there is a framework that is reasonably straightforward and put forward in the Secretary's recommendations that I think can serve as the strong basis for the crafting of appropriate legislation.

Mr. BURR. I thank you and I yield back, Mr. Chairman.

Mr. BILIRAKIS. Yield back. Mr. Markey who is not a member of the subcommittee——

Mr. EISSENBERG. Is there time for me to add something very quick?

Mr. BILIRAKIS. Very quick. He yielded back, you understand, time that he did not have.

Mr. EISSENBERG. The other area that is very important that we haven't talked about today is the quality of care area. And in some of the legislation that exists and in the Secretary's language we specify more clearly the kind of legal authority that would be provided for assuring quality of care and the need for personal information as well.

Mr. BILIRAKIS. Mr. Markey, who is not a member of the subcommittee but whom we respect greatly.

You are more than welcome, sir, to inquire.

Mr. MARKEY. Thank you very much, sir, and I thank you for your typical courtesy. You have always been gracious. I appreciate it very much.

This issue is, without question, the other side of the information-age coin. There is no question that because of rapid technological change and globalization that there are tremendous pressures upon our society to become more efficient. And the technology drives it and it makes it possible for consolidation across all industry lines, but it also creates other problems for individuals.

So what is good for a corporation is no longer necessarily good for individuals, although we can, in fact, find a way of reconciling the differences. So the truth of the electronic era is that there is a Dickensian quality to it. It is the best of wires, and the worst of wires simultaneously. It has the ability to enable and to ennoble and it has the power to degrade and to debase all at the same time.

The question for us is whether or not we want to animate the technologies with human values or just allow the technologies to take their own course knowing that without those values, that there will be a compromise of the individual.

And I think that we have to have this debate because I believe that we need the same values in the virtual world as we have in the real world, and only by debating these issues do we make sure that we separate the privacy keepers from the just curious peepers who increasingly, on-line, have the capacity to be able to move through all of our private lives.

And then you have this most dangerous of all categories, and that is the information reapers, that is, companies, corporations, software companies put together just to collect all this data and then to market it to a third party—to third parties, to sell it, to

sell our secrets, our health, our privacy, our financial services, any of our electronic transactions, children's transactions on-line.

All of it is valuable information. And so the question for us is whether or not we are going to act before the privacy pirates move in and create a new world that is very difficult for us legislatively to capture. My question to you, doctor, is the biotech industry has objected to imposing any privacy oversight over research which is privately funded.

Does privacy deserve less protection based on its source of funding, doctor? Is the IRB oversight process a significant barrier to good research? Isn't it true that many researchers view IRBs as helpful in ensuring research is doing well? Is there any reason why we can't extend the common rule in other words, to private research?

Ms. HAMBURG. As we have discussed already here this morning, we feel that the ongoing health and vitality of the research enterprise whether publicly supported or privately supported is critical to the future of our health care system and our Nation. But in order for that research enterprise to move forward, those participating in research have to have confidence and trust that their sensitive health information will be protected and that the data collected on them will be treated in a confidential and an appropriate way.

Clearly people participating in research are not looking to see where the funding comes from and will not be attuned to the specifics of privacy protections afforded in one context versus another. And we believe that we can achieve the goal of having both a healthy ongoing research enterprise and a set of privacy protections.

I think it is very important that we hear the concerns of people engaged in different types of research and in different contexts for the conduct of research, but that experience already has told us that you can move forward with good research, quality research.

Mr. MARKEY. Excellent, thank you.

Let me ask you this. Genentech's written testimony opposes any of the privacy legislation which is being proposed on our side. Mr. Waxman, myself, others moving forward are trying to get a debate on it, and they argue there is only minimal risk to human subjects.

Do you consider denial of health insurance a risk? Do you consider denial of a job a risk? Or should we just consider those minimal?

Ms. HAMBURG. I think it is clear, as your question suggests, that there are very serious consequences to the inappropriate divulging of certain sensitive health information and it is clear that we need to protect individuals. And it is ultimately in the interest of research to insure participants in the public-at-large that research activities are sensitive to those needs and address them.

Mr. MARKEY. Thank you, doctor.

Thank you, Mr. Chairman.

Mr. BILIRAKIS. I thank the gentleman.

Mr. BROWN. Mr. Chairman, could I ask unanimous consent for five additional questions?

Mr. BILIRAKIS. Without objection.

Mr. BROWN. Thank you.

Dr. Hamburg, I understand the Secretary doesn't have the authority to issue regulations as comprehensive as many of us on this panel—and perhaps you too, but many of us want to see addressed or are necessary. Spell out for us the areas, if you would, the Secretary's regulations can't cover that what we, in fact, want to protect?

Ms. HAMBURG. I think that with respect to the HIPAA privacy regulations, clearly it would be tied to information that is electronically managed, and we are still exploring the extent of what that means. But clearly tied to electronically managed data and also limited to a specific set of entities, providers, payers, and clearing houses, so that does limit the scope of the activity.

Mr. BROWN. So paper-based medical records, you cannot promulgate regulations to govern paper-based medical records.

Ms. HAMBURG. On exclusively paper-based. As I said, we are currently exploring the extent of our authorities, and so I cannot give you an absolute legally clear answer here, but it is very explicit information that is tied to electronically transmitted information.

Mr. BROWN. I think, Mr. Chairman, that speaks to the importance of—particularly since Congress has not addressed this issue comprehensively for 20 years or so, and it may not again in the near future, speaks to the importance of establishing—of moving forward with legislation, establishing a floor, and encouraging innovation in the States rather than establishing a ceiling and putting up a disincentive for State innovation.

I would like to yield for a couple of minutes to my friend from California, Mr. Waxman.

Mr. WAXMAN. Thank you very much. I think that last point you made was an excellent one because problems do come up that are not anticipated, and we ought to allow the Secretary or the States to go beyond minimum protections that we will have in Federal law. But the Secretary also called for private right of action to enforce the privacy provisions. Why do you think that is important?

Ms. HAMBURG. I think it is very important that individuals have an opportunity through the legal system to redress compromises to their privacy and confidentiality protections.

Mr. WAXMAN. If they don't have that legal right, it is a promise that may not come true?

Ms. HAMBURG. Well, I think that clearly if we are going to put forward a set of legal expectations about privacy protection and confidentiality, then we need to follow through with some teeth and there need to be, I think, both civil and criminal penalties for those who misuse or abuse information. And I think that individuals whose privacy has been compromised need some mechanism for redress.

Mr. WAXMAN. I thank my colleague for yielding. Mr. Chairman, I wonder if we could keep the record open and have them respond to questions that we may have.

By all means; we make a practice of that and if you would be willing to—I might ask if the gentleman would yield the balance of his time.

I guess I am not clear. I know Mr. Burr and others have asked about the preemption portion, the need for uniformity, et cetera.

And I realize maybe it is difficult for you to give us a yes or no answer.

I don't know how we could have uniformity to a point and then not preempt to another point; in other words, you are talking about this floor business.

Should we have uniformity where Federal law would preempt all State laws?

Ms. HAMBURG. I think there should be as I thought I had indicated earlier——

Mr. BILIRAKIS. You have said.

Ms. HAMBURG. I guess it is good I am not a lawyer.

Mr. BILIRAKIS. You sound like you would make a good one.

Ms. HAMBURG. There should be a set of clear standards that are in place that represent a uniform set of standards on a national basis, but then that represents a floor, not a ceiling, and does allow for State by State innovation based on changing circumstances, particular concerns.

Mr. BILIRAKIS. What you are saying is uniformity up to a point, but the States could—would not be preempted if they were to add to those uniform standards?

Ms. HAMBURG. This is, as you are very well aware, a complex set of issues that are being discussed in the context of a very complex health care system, a very complex set of research needs and requirements and, of course, a world where technology is changing rapidly. So we think that we need to maintain a certain level of flexibility, but there are important issues. And we need national legislation to address them.

Mr. BILIRAKIS. Couldn't we retain that flexibility on a national scale so that the flexibility can be done again on a national standpoint so that there would be complete uniformity?

I am not really expressing a position here. I am asking questions because I guess I am not clear given we have been working on this quite sometime.

Mr. WAXMAN. Would the chairman yield?

Mr. BILIRAKIS. Yes.

Mr. WAXMAN. I think there are times the States can see issues that affect them that may not affect people in other States like the HIV epidemic, for example, where we didn't anticipate such a thing before it happened.

When it happened, it hit certain States harder first than others. And a State might have wanted to add their own provisions, but under no circumstances do we want to have American citizens anywhere in this country not have certain basic protections of privacy of medical records.

So I think what you are saying—we do this all the time in Federal law—we are going to have certain provisions that will apply everywhere, and then States should be able to act when unanticipated issues come up. We don't want to tie their hands. They're closer to these problems than the people in the Federal Government. They can often be very innovative and we shouldn't stifle them.

Mr. BURR. Mr. Chairman, could I ask unanimous consent for one question?

Mr. BILIRAKIS. Without objection.

Mr. BURR. It really follows up, to some degree, on that, but you talked in your testimony about the sensitivity of genetic information. And I think one could conclude from your testimony that there might be a belief that there needs to be a different set of standards for genetic information than for everything else.

Ms. HAMBURG. Actually, we are not recommending that. We believe that if we can achieve a baseline that is appropriate and sufficiently comprehensive, it would embrace and protect for all kinds of health information and that it would be a mistake to begin to compartmentalize for the reasons we were just discussing about how things will emerge that we haven't thought about today.

Clearly today with all of the advances that are going on in the field of genetics, genetic screening is an area of great concern to the public, particularly because it is an area where science hasn't fully informed us—informed us about what some of the genetic screens actually mean.

So the potential for unintentional misuse as well as abuse is very, very clear and present now. And people are concerned about it, but there are many types of medical information that are sensitive. And we believe we should be striving for a comprehensive approach.

Mr. BURR. So you do see a uniformed approach. I thank you and thank the Chair.

Mr. MARKEY. Mr. Chairman, could I ask one additional question?

Mr. BILIRAKIS. After that nice note you just sent me, yes.

Ms. ESHOO. Mr. Chairman, could I just make a point of inquiry. Are we doing a second round of questions?

Mr. BILIRAKIS. No, we were not contemplating doing that although let's face it, that is what we are doing.

If you have something more by all means.

Ms. ESHOO. I think he should go first since he asked. But since we have done that, I would like to get mine in as well.

Mr. MARKEY. Thank you, Mr. Chairman. I will just ask one quick question.

Mr. BILIRAKIS. By all means.

Mr. MARKEY. Which is a clarification on the administration's position as to whether or not under existing law it has the ability to put a right of action on the books that can be exercised by individuals to protect their health care privacy.

Does the administration believe it has that legal authority under existing law or does it need new legislation in order to accomplish that goal?

Ms. HAMBURG. Certainly we believe it should be a part of whatever national legislation would be enacted, and we feel that in order to achieve the broad set of goals put forward in the Secretary's recommendation that is the right approach rather than to build on existing authorities.

Mr. MARKEY. The administration does not believe that it has authority under existing law?

Ms. HAMBURG. Under HIPAA?

Mr. MARKEY. Under any existing law.

Ms. HAMBURG. I don't know the answer to that question. There may be those in the department that do. We can get back to you on this.

Mr. MARKEY. I think it would be very important for the administration to clarify your position on the legal standing that you have on that issue before we proceed.

And I want to work with you, Mr. Chairman, through Mr. Brown who is the leader of the Democrats on these issues on the committee. I want to work through Mr. Brown with the majority toward, hopefully, a positive resolution.

Thank you, Mr. Brown, Mr. Chairman, for your indulgence.

Mr. BURR [presiding]. The gentleman's time has expired.

The Chair will recognize Ms. Eshoo.

Ms. ESHOO. Thank you. Mr. Chairman.

What kind of civil monetary penalties, criminal penalties or other provisions are in the Secretary's recommendations?

Ms. HAMBURG. The Secretary outlines in broad terms the concept of the requirements for civil penalties, civil monetary penalties for unauthorized disclosure of information and criminal penalties for the intentional abuse of information, release of information, and in keeping with actually what Congress mandated under HIPAA, the point was made that the penalties should be—well, perhaps we should get back to you in terms of the specific details because I am afraid I might not represent them appropriately.

Ms. ESHOO. That is more than fair.

I think it would be useful information if in fact there are specifics. If it just states that it should be or there are——

Ms. HAMBURG. It is broad in its approach, but it does indicate the need for both civil and criminal penalties under certain circumstances.

Ms. ESHOO. Thank you. Thanks again for each one of you being here today. Excellent. We learned a lot. This is exactly what a hearing should be about.

Thank you, Mr. Chairman.

Mr. BURR. I thank the gentlelady.

The Chair, seeing no requests for additional questions, would once again thank our three witnesses today and would dismiss the first panel and take this opportunity to call up the second panel.

Mr. BURR. The second panel is comprised of Dr. Steven Jacobsen with the Mayo Foundation; Dr. Robert Amdur, associate professor and chairman, Dartmouth Committee for the Protection of Human Subjects, Dartmouth Medical School; David Stump, Genentech Fellow; Ms. Fran Visco, president, National Breast Cancer Coalition; Ms. Dawn Gencarelli, Harvard Pilgrim Health Care; Ms. Abbey Meyers, National Organization of Rare Disease; Daniel Krinsky, Patient Services and Pharmacy Practice; and Terry Latanich, Government Affairs, Merck-Medco.

The Chair would like to welcome our witnesses that comprise the second panel. We realize it is rather large. I would ask all of our witnesses today to try to hold their opening statements to the 5-minute rule. We will attempt to try to figure out what is going on on the House floor. I would ask all members to try to limit to one round of questioning if we can, but certainly the Chair would entertain any requests for clarification.

At this time if I may, I will just start at my left—the Chair has changed his mind. I will start at my right with Dr. Jacobsen is recognized.

STATEMENTS OF STEVEN J. JACOBSEN, DIRECTOR, SECTION OF CLINICAL EPIDEMIOLOGY, THE MAYO FOUNDATION; ROBERT AMDUR, FORMER ASSOCIATE PROFESSOR OF MEDICINE AND CHAIRPERSON, DARTMOUTH COMMITTEE FOR THE PROTECTION OF HUMAN SUBJECTS, DARTMOUTH MEDICAL SCHOOL; DAVID C. STUMP, GENENTECH FELLOW; FRAN VISCO, PRESIDENT, NATIONAL BREAST CANCER COALITION; DAWN M. GENCARELLI, MANAGER, HEALTH POLICY, HARVARD PILGRIM HEALTH CARE; ABBEY MEYERS, PRESIDENT, NATIONAL ORGANIZATION OF RARE DISORDERS; DANIEL L. KRINSKY, DIRECTOR, PATIENT SERVICES AND PHARMACY PRACTICE, RITZMAN PHARMACIES INC.; AND TERRY S. LATANICH, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, MERCK-MEDCO

Mr. JACOBSEN. Mr. Chairman, members of the committee, I am Dr. Steve Jacobsen, a physician researcher at Mayo Clinic. I want to thank you for the opportunity to testify about the importance of medical records base research and the potential impact of legislation restricting access to medical records for this category of research.

For the past 8-years, I have had the privilege to work at the Mayo Clinic. I truly believe that Mayo Clinic's international reputation as a center of excellence grew out of its commitment to improve patient care through research, often through the use of the medical record. Our founders, Dr. William and Charles Mayo went on record early in this century saying the best way to improve care was to rigorously evaluate patient outcomes.

They and their colleagues designed systems that ensure that all information about a patient was immediately available for care and readily accessible for systematic reviews of the outcomes of care. They set a precedence for the scores of studies of the outcomes of care that have changed medical practice at Mayo Clinic and throughout the world.

I also need to stress that Mayo Clinic maintains its commitment to the confidentiality of medical information. One of our most basic tenets is that information is available because of the trust between the patient and the providers of care. All employees are instructed on the importance of confidentiality.

In regard to medical record-based research, I want to emphasize that information from this type of research is vital to patients and their physicians. This is not an issue of society's need for information versus the patient's right to privacy. Patients, individually, have a great need for this information. Let me give you an example.

I have a friend who was recently diagnosed with prostate cancer. Upon hearing of the diagnosis, he immediately had a number of questions. What was going to happen to him? What were the chances of complications? Were there things his sons should know about their risk of developing the disease?

I am sure you can think of similar questions that you have wanted to ask your own physician. The answer to these questions are often obtained by reviewing medical records. It is because of the importance of answering these types of questions for patients and

their physicians that Mayo Clinic maintains its commitment to accurate medical record-based research.

My second point is that each and every one of us in this room needs to be concerned about the potential impact of legislation that might block access to some medical records for research. This concern comes from the threats of the accuracy of findings of studies that can result from missing some records. To illustrate, let me go back to my friend.

One of the important factors in his decision about surgical therapy was the risk of certain side effects. Imagine if over the past several years men who experienced those side effects were upset with their outcome. Maybe they didn't expect it. Perhaps they blame their surgeon but regardless refuse access to the medical record for research purposes.

A study based only on patients who did provide the authorization, in other words, those who did not experience those side effects, would suggest that the surgery was much safer than in reality. Thus, my friend could have made a decision on the basis of this information.

This potential inaccuracy is the crux of our concern for limiting access to medical records for research purposes. At Mayo Clinic we feel it our responsibility to provide patients and their physicians the best possible information so the best possible decisions can be made.

Is this threat real? I believe the answer is yes. As you know, the State of Minnesota now limits access to medical records for research except with prior authorization. In a recent study, we found that refusal rates were higher among women, persons under 6 years of age, and persons with certain underlying illnesses such as mental disorders, breast cancer, and reproductive problems. Unfortunately, the degree of inaccuracy resulting from the absence of such records is probably not knowable in any particular study. The only way to ensure accurate information is through a complete and unbiased conclusion of all medical records of all appropriate patients.

Finally, the third point I would like to make relates to potential harm if the rules regarding research use of medical records vary from State to State. The biases imposed as a consequence of different laws could seriously hinder the improvement of patient care. For example, in a study of the outcomes of prostate cancer surgery in patients from the Mayo Clinic sites in Arizona, Florida, and Minnesota, it could be virtually impossible to sort out if any observed differences in the outcomes of these patients were due to different patient characteristics, different processes of care, or simply biases introduced by the different laws. It is extremely important that laws concerning the research use of medical records are uniform across all States.

In closing, I would like to emphasize that medical record-based research is vital to the continued improvement of patient care and is essential to patients and physicians as they consider decisions about the courses of care. This information must be as accurate as possible.

The only way to ensure this is through complete and unbiased information. We do recognize the need for confidentiality of infor-

mation, but we must not confuse research access with open access to medical information.

Mr. Chairman, the restriction of these medical records for research purposes does not ensure privacy of personal medical information. It does not address the public's concern with regard to the potential misuse of health information. Instead it hinders medical research as directed toward improved patient care and puts the public's health and well-being at risk.

Thank you.

[The prepared statement of Steven J. Jacobsen follows:]

PREPARED STATEMENT OF STEVEN J. JACOBSEN, ASSOCIATE PROFESSOR OF EPIDEMIOLOGY, MAYO CLINIC

Chairman Bilirakis, members of the committee, I am Dr. Steve Jacobsen, a physician researcher at Mayo Clinic. Thank you for the opportunity to testify before you regarding the important issue of medical records confidentiality.

Today, I would like to discuss two fundamental questions bearing on this issue. The first is: What is the importance of medical records-based research to the public? And the second is: What is the impact of legislation restricting access to medical records on this category of research?

For the past eight years, I have been privileged to work at the Mayo Clinic. I truly believe that Mayo Clinic's international reputation as a center of excellence in medicine and surgery grew out of its commitment to improve patient care through research, often through the use of the medical record. In fact, our founders, Drs. Will and Charlie Mayo went on record in the early years of this century saying that the best way to improve care was to rigorously evaluate patient outcomes. In order to do this, they and their colleagues designed a "unit medical record" in which medical data on each patient is stored in one self-contained packet that is kept in perpetuity. This was done so that all information about a patient was immediately available to the physician treating the patient and so that a systematic review of the outcomes of care could be performed easily. They also built indexes that identified records of patients with specific conditions or who had undergone specific procedures. They recognized that there was a wealth of information collected as part of routine clinical care and that no subset of this information could be conceived that would capture sufficient detail for all potential studies. Through these efforts, they set the precedent for the scores of studies of the outcomes of care that have changed medical practice at Mayo Clinic and throughout the world.

Medical records research is vital to maintaining and improving the health of the American public. In fact, virtually every health hazard that we know of today has been identified using information from medical records. Take AIDS, for example. If researchers had not been allowed to study the medical records of patients with unusual immune deficiency problems in the late 1970's, the characterization of the AIDS epidemic would have been delayed at a substantial cost to the public's health. Other examples include studies examining the benefits and risks of estrogen treatment, as well as the health risks of smoking, dietary fats, obesity, and certain occupations. You may have read that an outbreak of invasive streptococcal infection was identified at Mayo in 1995. Without access to the medical records of patients with these unusual infections, characterization of this syndrome and isolation of this deadly bacterial strain would have been delayed. And over one hundred school children—which our research showed were the unwitting carriers of this deadly germ in their throats—would have gone untreated. This discovery led to the designation of invasive strep as a reportable disease. Such a designation permits earlier recognition and control of epidemics. Medical records research is also critical for evaluating the long-term side effects of drugs, the safety of medical devices or procedures, the cost effectiveness of alternative medical practices, and the usefulness of diagnostic tests.

Mayo Clinic, as I mentioned, is committed to improving the practice of medicine and patient care though its long-standing tradition of performing these types of studies, looking at groups of patients. This approach is important because physicians may remember patients who have done well with a particular treatment. Likewise, they can remember the patients who have not. However, they cannot remember these results in sufficient detail to quantify the likelihood of a good or bad result. We use systematic studies of groups of patients so that we can sort out true differences from random outcomes. Furthermore, when we perform these studies, we

have to be sure that the findings reflect any true differences and not just the factors related to which medical records were reviewed. I will expand on this in a moment.

Before doing so, however, I need to stress the point that Mayo Clinic also maintains its commitment to the confidentiality of medical information as well. It is one of our most basic tenets that this information is available because of the trust between the patient and the providers of care. All employees are instructed on the importance of confidentiality; there are strict penalties, including loss of employment, for violations of this trust.

As part of this, we strongly maintain that research access IS NOT open access to the medical record. All studies are monitored by our Institutional Review Board. Information is collected from the medical record by trained individuals, usually just one or two for any given study. All of these individuals have been thoroughly briefed about the importance of confidentiality and procedures to help ensure it. The information is summarized and never published in identifiable form. This is not casual access.

As you consider legislation concerning research use of medical records, there are several important factors that I hope you will take into account. These include the importance of medical record research, the potential impact of legislation blocking access to some medical records, and the importance of consistency in the laws across all states.

First, it is important to understand that information from medical record research is vital to patients and their physicians. Most advocates of increased restrictions paint the issue as one of society's need for information versus the patient's right to privacy. However, the patients, themselves, have a great need for this information. Let me give you an example. I recently had a friend who was diagnosed with prostate cancer. Upon hearing of the diagnosis, he immediately had a number of questions. What is going to happen to me? Among each of the treatments, what are the long-term outcomes? Are there things I should tell my sons about their risk of developing this disease? I am sure that if you think back to your own encounters with the medical system, you can think of when you have asked some of those same types of questions. These kinds of questions can only be answered by studying the experience of large groups of patients. It is because of the importance of answering these questions for patients and their physicians that Mayo Clinic maintains it commitment to accurate medical record research.

The second point is that we all need to be concerned about the potential impact of legislation that might block access to some medical records for research purposes. This concern comes from the potential threats to the accuracy of findings of studies due to incomplete ascertainment of outcomes. To illustrate, let me go back to my friend recently diagnosed with prostate cancer. One of the important factors in his decision about whether or not to undergo surgical therapy was the risk of certain side effects. Imagine what would happen if, over the past several years, men who experienced the side effects were upset with their outcome, perhaps blamed their surgeon, and refused access to medical record for research purposes. A study based only on those patients who did not experience those side effects would suggest that the surgery was much safer than in reality. Thus, my friend would be making his decision on the basis of misinformation.

This potential threat is the crux of the concern for limiting access to medical records for research purposes. At Mayo Clinic, we feel it our responsibility to provide patients and their physicians the best possible information so that the best possible decisions can be made.

Is this threat real? I believe the answer is "Yes". I was principal investigator of a study recently published in the *Mayo Clinic Proceedings,* a copy of which is included in the Appendix to my written statement. We conducted this Institutional Review Board approved study to compare the characteristics of persons refusing to provide a general authorization of the use of medical record for research purposes with those who did. This was prompted by passage of a law in the State of Minnesota that limits access to medical records for research except with the prior authorization of the patients in question. Institutionally, we felt it necessary to understand the potential impact of the recent Minnesota bill on the quality of information generated from medical record studies.

In this study among patients recently seen at Mayo Clinic, we found that slightly over 3% of patients explicitly told us "I do not authorize Mayo to review medical records about me for medical research". Approximately 80% of patients provided us an explicit authorization and 17% did not explicitly give us an indication of their wishes despite three written contacts. This demonstrates the importance of how the response of persons not explicitly expressing their wishes are treated. If considered a "No", the effective refusal rate would have been over 20%. This high proportion

greatly increases the chance that a bias such as I described in the hypothetical example, could influence the results of any study.

Another important finding was that refusal rates were higher among certain subgroups. In general, women were more likely to refuse authorization than men, persons under 60 years of age were more likely to refuse than older individuals, and patients traveling longer distances for care at Mayo Clinic were less likely to refuse than those from the local community. In addition, we found that persons with certain underlying illnesses, such as mental disorders, breast cancer and reproductive problems were also more likely to refuse authorization. While some of these findings may be somewhat predictable, it is not possible to know how refusal rates might systematically differ between any particular comparison groups. Furthermore, it is likely that our assessment of potential differences underestimates what would likely be happening at other institutions that don't enjoy the same level of trust and respect from their patients. The bottom line is that the degree of inaccuracy introduced by restricting access to medical records for research purposes is probably not knowable in any particular study and is likely to vary from question to question and from setting to setting. The only way to ensure accurate information is through complete and unbiased inclusion of all medical records.

Finally, this third point that I would like to make relates to the potential harm of allowing the rules regarding research use of medical records to vary from state to state. Mayo Clinic Rochester is about 60 miles west of the Wisconsin border and 40 miles north of the Iowa border. Thus, a substantial proportion of our referral practice comes from these two neighboring states. In fact, Mayo operates in five states. Imagine if you will, the complexity of trying to deal with three separate sets of laws, each with different standards for the use of medical records for research purposes. More important, however, is the concern for different sets of biases imposed as a consequence of these laws. For example, imagine a study comparing the outcomes of prostate cancer surgery in patients from the University of Iowa and Mayo Clinic Rochester. If different laws affected the selection factors for this study, the results would be extremely difficult to interpret. It would be virtually impossible to sort out if any observed differences were due to patient characteristics, processes of care, or simply biases introduced by different laws controlling access to medical records for research purposes. This might preclude the investigator's ability to identify certain patient characteristics or patterns of care that may benefit patients with prostate cancer. It is extremely important that laws concerning the research use of medical records are uniform across all states.

In closing, I would like to emphasize that medical record research is vital to the continued improvement of patient care. Furthermore, information generated from medical record research is essential to patients and physicians as they consider decisions about courses of care. Consequently, it is absolutely essential that this information be as accurate as possible. The only way to ensure this is through complete and unbiased information. At the same time, it is important to recognize the need for confidentiality of information. We mustn't, however, confuse research access with open access to medical information. Mr. Chairman, legislation restricting access to medical records for research purposes does not ensure privacy of personal medical information and does not address the public's concerns regarding the potential misuse of public health information. Instead, it hinders scientific research and puts the public's health and well-being at risk for serious harm. Your attention should be focused on stopping the actual abuses of medical record information that harms patients.

Thank you for your attention.

Mr. BURR. Thank you, Dr. Jacobsen.

The Chair would recognize Dr. Amdur for 5 minutes.

STATEMENT OF ROBERT AMDUR

Mr. AMDUR. Good morning. I am a physician with an interest in research ethics. I am here to urge you to pass legislation that will require that research involving review of confidential information from a person's medical record be held to the same ethical standards regardless of who conducts the research or where the funding comes from.

Most of the medical research that I perform requires confidential information from medical records, so I know how important it is to have access to this kind of information.

I have experience with the Federal regulations related to research because for the past 4 years I have chaired the institutional review board at Dartmouth. For anybody not familiar with that term, an institutional review board is a type of ethics committee that is charged with protecting the rights and welfare of research participants.

When considering medical records legislation as you are, it is important to understand two main points. The first point is that our society currently has only one formal system for evaluating the ethics of a research study. And this is the system of protection described in our code of Federal regulations. These regulations basically present a manual that explains the procedure and criteria that should be used to determine if a specific research proposal is acceptable from the ethical standpoint. The basic criteria for ethical research are common sense things like being sure that the risks to subjects are minimized and that the risks are in proportion to the expected benefits of the research.

The take-home message that I would like to leave you with is that the Federal regulations are good regulations and are to help to protect individual subjects and to maintain the integrity of our research process. However, what many people don't understand is that without Federal legislation—the protections that are provided by these regulations are limited to studies that are funded by a Federal agency or being done as part of an application for FDA licensure.

Today, if I want to study the medical history of congressional representatives like yourself, I don't need to get Federal funds, I can finance it myself. I may be able to get access to your medical records without going through any meaningful review process. That is the problem.

The final point that I would like to make is a response to the arguments that I have read about passing legislation about medical records research. As I see it, the main issue of concern is that if we require the same standard for both privately and federally funded research, the volume of regulated activity will increase to the point that society's ability to conduct research will be compromised.

I don't share this concern, and I think that it reflects a fundamental misunderstanding in two basic areas. One misunderstanding is that there is currently a lot of privately funded research going on outside the Federal regulatory system. This is not true.

While we don't have definitive data on this issue, the fact of the matter is most privately funded research is done either as part of an FDA application for licensure which means it must comply with Federal regulations or at academic institutions which have signed a type of contract with the National Institutes of Health called a multiple project assurance.

What this contract says is that the institution will require that all research under its auspices be done in compliance with Federal regulations, regardless of funding source. The point is that the great majority of privately funded research today is already going on in compliance with Federal regulations and reviewed by the IRB system.

The second misunderstanding is that extending the authority of the Federal regulations to privately funded research will mean that medical centers, insurance companies, et cetera, throughout the country will have to go through the institutional review board system every time they want to review medical records as part of a quality assessment effort, utilization review, outcome evaluation, et cetera.

This is not going to happen because the regulations only apply to medical research. Medical research in the regulations is defined to be, "a systematic investigation designed to develop or contribute to generalizeable knowledge," a specific definition. There is no question that the institutional review board authority does not extend to the wide range of non-research activities that opponents of the effort are concerned about.

Thank you.

[The prepared statement of Robert Amdur follows:]

PREPARED STATEMENT OF ROBERT AMDUR, FORMER ASSOCIATE PROFESSOR OF MEDICINE, DARTMOUTH MEDICAL SCHOOL

Introduction

Good morning. My name is Robert Amdur. I am a physician with an interest in research ethics. I am here to urge you to pass legislation that will require that research that involves review of confidential information from a persons medical record be held to the same ethical standard regardless of who directs the research or where the funding comes from. Most of the medical research that I do requires confidential information from medical records so I know how important it is to have access to this kind of information. I am familiar with federal research regulations because I have chaired the Institutional Review Board at Dartmouth for the past 4 years. For those of you who are not familiar with this term, the Institutional Review Board is a type of ethics committee that is charged with protecting the rights and welfare of research subjects.

Main Points

When considering medical records legislation it is important to understand two main points:

1. The first point is that our society currently has only one formal system for evaluating the ethics of a research study and this is the system of protections described in our code of federal regulations. These regulations basically present a manual that explains the procedure and criteria that should be used to determine if a specific research proposal is acceptable from the ethical standpoint. The basic criteria for ethical research are common sense things like being sure that the risks to subjects are minimized and that risks are appropriate in relation to the expected benefits. The take home message is that these are good regulations that help to protect individual subjects and maintain the integrity of the research process. However, what many people don't understand is that without federal legislation the protections that are provided by these regulations are limited to studies that are funded by a federal agency or being done as part of an application for FDA licensure. Today if I want to study the medical history of congressional representatives, and I don't use federal funds, I may be able to get access to your medical records without going through any meaningful review process.

2. The final point that I would like to make is a response to the argument against passing legislation about medical record research. As I see it, the main issue of concern is that if we require the same standards for both privately and federally funded research, the volume of regulated activities will increase to the point that the ability to conduct research will be compromised. I do not share this concern and I think it reflects a misunderstanding in two areas.

One misunderstanding is that there is currently a lot of privately funded research that is being done outside the federal regulatory system. This is not true. Most privately funded research is done at institutions that sign a type of contract called a "Multiple Project Assurance" with the National Institutes of Health that commits them to conducting all research according to federal regulations regardless of funding source. I am happy to explain why an institution would want to establish this Assurance in the question period, but for the purpose of this discussion the point

is that passing federal legislation will not meaningfully increase the volume of regulated research because most privately funded research is already being reviewed according to federal regulations.

The second misunderstanding is that extending the authority of the federal regulations to privately funded research will mean that medical centers throughout the country will have to go through the Institutional Review Board system every time they want to review medical records as part of a quality assessment or utilization review activity. This is not going to happen because the regulations only apply to medical record review that is being done for research purposes. As the regulations define research to be "a systematic investigation designed to develop or contribute to generalizable knowledge" there is no question that Institutional Review Board authority does not extend to the wide range of non-research activities that opponents of federal legislation in this setting are concerned about.

Mr. BURR. Thank you, doctor.

The Chair would recognize Dr. Stump for 5 minutes.

STATEMENT OF DAVID C. STUMP

Mr. STUMP. Good morning, Mr. Chairman, members of the committee.

Thank you for the opportunity to testify before you today regarding this most important issue of confidentiality of patient medical information.

My name is David Stump. I am a physician and vice president of clinical research for Genentech, Incorporated, a San Francisco, California-based biotechnology company. Genentech is the pioneer in the biotech field responsible for the development of several breakthrough, life-saving biological products, including Pulmozyme for cystic fibrosis; Activase for the treatment of heart attack and stroke; Rituxan for the therapy of non-Hodgkins lymphoma; and most recently, Herceptin, a new treatment for metastatic breast cancer.

Genentech has been working for several years in support of enactment of strong uniform Federal standards designed to safeguard the confidentiality of patient health information and limit its use to activities which are appropriate and necessary to the daily functioning of our dynamic health care delivery system, including the use of information for biomedical research.

Throughout this effort, however, we have grown to realize that while such Federal standards are clearly needed to help assuage concerns over the abuse of patient health information and facilitate patient confidence in the system, it is equally critical that new Federal law recognize that patient information is the foundation of our growing effort to enhance the quality of health care we deliver through accountability, outcomes analysis, and medical research. Any failure to strike this delicate balance could have the dramatic and unintended consequence of stifling innovation and limiting the ability of companies like Genentech to effectively continue its mission in pursuing drug therapies for unmet medical needs.

In addition, any new Federal standards must create a single uniform system of safeguards, accountability, and penalties by which the research community must abide by preempting the increasing patchwork of State law which is working to minimize our ability to conduct research effectively and affordably.

I understand that this is a first hearing of this subcommittee and that you face an August deadline for action. While you will no doubt hear about the importance of this issue from many other

panels today, I personally want to emphasize the critical importance of your decisions regarding patient confidentiality to the biomedical research community and to the patients who suffer from the illnesses we seek to study and cure.

While we at Genentech are firmly committed to protecting the confidentiality of every single patient whose information we review and use each minute of each day, our ability to hypothesize, study, develop, test, and manufacture new products is directly related to both the quality and availability of information.

Our founders were the first to conceptualize the process of cloning human proteins for the purpose of manufacturing life-saving therapies. Vital to this process then and now, nearly 20 years later, is the ability to access patient data past, present, and future. Please understand that I will not testify today that new Federal standards that limit our ability to access patient data will eliminate biomedical research as we now know it.

However, I will say without responsible access to such information, patients themselves whom we all seek to protect will be the ultimate losers as they will have access to fewer important new therapies.

The medical research community depends upon uniform standards for the performance of clinic and medical investigations. As we consider new important legislation aimed at protecting the privacy and confidentiality of patients from abuse, we need to be certain that this legislation does not erect unnecessary barriers that will slow and impede medical research. To do so will adversely impact all future generations who are dependent on the steady progress of medical research in order to improve their lives as they encounter and struggle with consequences of illness and disease.

The United States is unquestionably the world's leader in medical research. Our leadership to date has been fostered by ready, uniform access to key information and data contained in the patient's medical records. Our own clinical studies involve data from patients all over the country and the world, for that matter. We engage in partnerships with research entities, health plans, and others located across all 50 States of the United States.

I know that access to data drives research, particularly medical research, and access to patient's data has driven medical research in the United States since the turn of the 20th century. Of particular concern to us are proposals that would extend Federal oversight into private research where the research involves information only and not the patients themselves.

Unfortunately, legislation introduced recently would accomplish this by extending the common rule to all research, meaning that even our data and archival research would be subject to review by an institutional review board. This is problematic to us for a number of reasons.

First, the IRB rules and policies surrounding informed consent are intended to ensure that human subjects participating in clinical trials are made sufficiently aware through the informed consent process of the potential risk of their safety. Thus, the rules are intended to ensure the safety of the human subject.

This legislative debate is about the use of medical information. The health safety risks to the human subject presented by con-

fidential review and use of medical information is minimal thus the application of the common rule and of IRB review to private, archival data review is an apples to oranges comparison.

Thank you, Mr. Chairman, for allowing me to share with you some of Genentech's principles and concerns regarding patient confidentiality. The subcommittee has been a vital partner in assuring a stable and fruitful environment for biomedical research as illustrated by your recent efforts on the Food and Drug Administration Modernization Act.

Please understand that the ultimate impact of this issue is no different and is directly related to our ability to continue innovative research. Please be assured that we share your commitment to protecting and safeguarding patient information. After all, patients are ultimately our business.

Please also understand that information is a lifeblood of research. We applaud this subcommittee's effort and very much look forward to working with you and others toward the final enactment of strong, workable and, most importantly, uniform Federal standards protecting the confidentiality of patient medical information.

Thank you.

[The prepared statement of David C. Stump follows:]

PREPARED STATEMENT OF DAVE STUMP, VICE PRESIDENT, CLINICAL DEVELOPMENT & GENENTECH FELLOW, GENENTECH, INC.

Good morning, Mr. Chairman, and Members of the Committee. Thank you for the opportunity to testify before you today regarding this most important issue of the confidentiality of patient medical information. My name is Dr. Dave Stump, and I am Vice President of Clinical Development for Genentech, Inc., a San Francisco, California-based biotechnology company. Genentech, Inc. is a pioneer in the biotechnology field, responsible for the development of several breakthrough, life-saving biological products, including Pulmozyme for Cystic Fibrosis; Activase for cardiac disease; Rituxan, for non-Hodgkins lymphoma; and most recently, Herceptin for metastatic breast cancer.

Genentech, Inc. is an active member of the Pharmaceutical Research and Manufacturers of America (PhRMA), the Biotechnology Industry Organization (BIO) and the Healthcare Leadership Council (HLC). We have been working closely with these organizations and numerous other coalition partners through the HLC in support of enactment of strong, *uniform* federal standards designed to safeguard the confidentiality of patient health information and limit its use to activities which are appropriate and necessary to the daily functioning of our dynamic health care delivery system, including the use of information for biomedical research.

Throughout this effort, however, we have grown to realize that while such federal standards are needed to help assuage concerns over the abuse of patient health information and facilitate patient confidence in the system, it is equally critical that new federal law recognize that patient information is the foundation of our growing effort to enhance the quality of health care we deliver through accountability, outcomes analysis and medical research. Any failure to strike this delicate balance could have the dramatic and unintended consequence of stifling innovation and limiting the ability of companies like Genentech, Inc. to effectively continue its mission and pursuit of drug therapies for unmet medical needs. In addition, any new federal standards must create a single, uniform system of safeguards, accountability and penalties by which the research community must abide by preempting the increasing patchwork of state law which is working to minimize our ability to conduct research effectively and affordably.

I understand that this is the first hearing of this Subcommittee, and that you face an August deadline for action. While you will no doubt hear about the importance of this issue from all of the other panelists today, I want to emphasize the importance and saliency of your decisions regarding patient confidentiality to the biomedical research community and to the patients who suffer from the illnesses we study. While we at Genentech, Inc. are firmly committed to protecting the confidentiality of the patient information we review and use each minute of each day, our

ability to hypothesize, study, develop, test and manufacture products is directly related to the quality and availability of information.

Our founders, Herb Boyer and Bob Swanson, were the first to conceptualize the process of cloning human proteins for the purpose of manufacturing life-saving therapies. Vital to this process then and now, nearly 20 years later, is the ability to access patient data—past, present and future. I will not testify today that new federal standards that limit our ability to access patient data will eliminate biomedical research as we know it. I will say, however, that without responsible access to such information, patients will be the true losers as patients will have access to fewer, more expensive therapies.

The medical research community depends upon uniform standards for the performance of clinical and medical investigations. As we consider new important legislation aimed at protecting the privacy and confidentiality of patients from abuse, we need to be certain that this legislation does not erect unnecessary barriers that slow and impede medical research. To do so will adversely impact all future generations who are dependent on the steady progress of medical research in order to improve their lives as they encounter and struggle with the consequences of illness and disease.

The United States is unquestionably the world's leader in medical research. With appropriate pride, we can point to our academic research institutions, the National Institutes of Health (NIH) and the Center for Disease Control (CDC), to name a few of the more prominent institutions. The United States is home to leaders in all types and varieties of medical research from epidemiology and outcomes research on one hand to the application of novel surgical techniques on the other. Our leadership, however, has been fostered by ready, uniform access to the key information and data contained in the patient's medical records. Our studies involve data as well as patients from all over the country, and the World, for that matter. We engage in partnerships with research entities, health plans and others also located across the 50 United States. I know that access to data drives research, particularly medical research, and access to patient's data has driven medical research in the United States since the turn of the 20th century.

Of particular concern to Genentech, Inc. are proposals that would extend federal oversight into private research where the research involves information only, and not the patients themselves. Legislation introduced by Representative Markey (D-MA) (H.R. 1057) accomplishes this by extending the Common Rule to all research, meaning that even our data and archival research would be subject to review by an Institutional Review Board (IRB). This is problematic for a number of reasons. First, the IRB rules and policies surrounding "informed consent" are intended to ensure that human subjects participating in clinical trials are made sufficiently aware, through the informed consent process, of the potential risks to their safety. Thus, the rules are intended to ensure the safety of the human subject. This legislative debate is about the use of *medical information.* The "risks" to the human subject presented by review and use of medical information is minimal and thus, the application of the Common Rule and of IRB review to private, archival data review is an apples-to-oranges comparison.

Further, I understand that IRBs do actually review archival research projects of institutions which are otherwise subject to the Common Rule. However, in those circumstances, the rule provides for expedited review of such research as it is considered to present "minimal risk" to the individual. Even the suggestion that we would be able to obtain expedited review of our archival research projects would add significant new layers of unnecessary federal oversight over private activities, depleting time and resources from our research endeavors. What appears to be a simple, straightforward requirement would directly result in fewer projects being initiated and fewer products being discovered. Conversely, we support an approach which would impose accountability on our ability to access information, limit our use of such information to bona fide research, and impose penalties on us for its misuse.

Thus, workable and uniform rules regarding how we may access and use this gold mine of information are critical to our underlying success. Let us consider some examples:

1. The Mayo Clinic was founded in 1907. The founders recognized the value of looking critically at their own experience, both in terms of the natural history of disease in their patients and the outcomes of their surgical and medical interventions. The Mayo Clinic has been a leader in the indexing of medical records, the application of the information technologies needed to search and retrieve information from their patient databases, and in outcomes research. Dr. Melton described some of the Mayo Clinic experience in an editorial in *New England Journal of Medicine* in 1997. He noted that more than 1,000 articles have been published in the medical literature based on the Mayo Clinic experience, and

described particular difficulties associated with a law passed in Minnesota which has made it more difficult for the Mayo Clinic to conduct epidemiologic research by requiring specific patient authorization for the use of patient data.

Now that the Mayo Clinic has spread to at least three states (Florida, Arizona, and Minnesota), and is a pioneer in the development of a computerized medical record, we can look forward to even more productive information stemming from their experience, assuming that ill-advised legislation from states or the federal government relating to patient confidentiality does not dramatically erode our ability to use this information to further medical research.

2. The comparison of medical research done in the United States and Europe by pharmaceutical companies reveals some important insights. The United States is a preferred site for drug development. I believe this relates to the presence of uniform standards for pharmaceutical research supervised by the FDA as well as to the similar guidelines adopted by physicians and institutions in the United States. Compare our situation to the diverse array of regulatory agencies one encounters in Europe, not to mention the variations in language, culture, politics, and standards of medical practice. The implementation of different local standards of patient confidentiality in the United States will have the practical effect of erecting barriers to medical investigations of all kinds. Ultimately, these barriers will lead to inefficiency and a loss of the advantages now present in our country. Pharmaceutical companies care deeply about time, resource expenditures, and productivity. Should legislation lead to disincentives for pharmaceutical research, drug development efforts may well be shifted away from the United States towards more favorable environments.
3. Recently the National Registry for Myocardial Infarction (NRMI) showed that important differences exist between different regions of the United States in regard to the diagnosis and treatment of myocardial infarction or heart attacks. Women in general, and older women in particular, were much less likely to have their heart attack diagnosed and treated as compared to men. These differences varied significantly by region in the US. Uniform standards allow "outcomes research" to be done across our country and detect deviations that can be addressed. This type of research is critical for improving the quality and reducing the cost of treatment and care.

In the past few years significant progress has been achieved in the understanding of genomics in the metabolism of drugs and in drug interactions. The importance of drug metabolism was initially recognized as differences in pharmacokinetics and pharmacodynamics in racial sub-populations. Subsequently, the differences have been attributed to the genetic variations such as cytochrome P450 that are responsible for the metabolism of drugs. These differences are critical to understanding the safety and efficacy of many drugs across patient populations. The study of relevant sub-populations has become a common FDA requirement for the approval of many drugs. The majority of some of these sub-populations are concentrated in a few states. State regulations inhibiting access to patient records will have the unintended consequence of inhibiting access to information about the sub-populations of patients. As a result, we will know less about their diseases, the natural history of diseases in these subgroups, and the effects of medical and surgical treatment on their illnesses.

This is not just a theoretical argument. In the 1960's and 1970's, we routinely excluded women and children from research involving new drugs to "protect them." As a result, we had almost no information about the safety and activity of these drugs in women or children. Despite the absence of critical information, these same drugs were broadly used in the treatment of women and children once they were approved.

Another example is the FDA's regulations for filing an Investigational New Drug Application (NDA) prior to commencing studies in humans. This is a significant hurdle that is not present in the United Kingdom where research can be done on normal male volunteers with informed consent and approval from an Institutional Review Board (IRB). Many pharmaceutical companies, even those centered in the United States, are performing initial human studies in the United Kingdom. I maintain that unnecessary barriers create real disincentives for doing medical investigations and fewer investigations are not in the patient's best interests. Clearly, we need to avoid legislation that will produce similar unintended consequences in the future.

The economic rationale for a uniform standard for patient confidentiality is compelling. Diverse laws governing patient confidentiality will create a need for individually "tailored" programs aimed at gaining access to the data in patient's records. The variability and diversity between different states will create a level of unnecessary complexity. To address the complexity, researchers will need to spend more

time and more money to accomplish their research goals. The consequences will be to increase the cost of research and reduce the number of investigations that are done. Smaller numbers of more expensive studies are not in the best interests of patients or our country.

To put this discussion in context, Genentech, Inc., as well as the HLC coalition, support the general approach taken in legislation introduced in April by Senator Bennett (R-UT). Senator Bennett's bill, the "*Medical Information Protection Act of 1999*," provides for comprehensive standards relating to patient confidentiality and imposes clear limits on the ability to use information for purposes of health care delivery and medical research. Yet, the bill establishes standards in a way that provides sufficient flexibility for each health plan, researcher, physician and hospital to establish its own system for ensuring compliance. Further, the bill provides very thorough preemption of state law, creating a uniform, predictable environment for the research community while replacing current state law with a rational, comprehensive system of federal safeguards, responsibilities, limits and penalties. To date, this is the only legislative proposal that would effectively address concerns I described earlier, such as those of the Mayo Clinic, while not sacrificing any "protections" provided to patients.

Conversely, the proposal introduced by Representative Markey would undermine our ability to conduct broad, inclusive, population-based research using patient data by subjecting us to a new federal standard as well as several conflicting state law standards relating to use, safeguards and patient authorization. Specifically, the Markey proposal would not only expressly extend federal oversight into all private research activities involving only information, the proposal also would establish a federal "floor," allowing any state law which is considered to provide "greater protection" than the federal law to remain in effect. Even disregarding the practical difficulty of determining such a subjective standard as what constitutes "greater protection," which would undoubtedly require litigation to mediate, this standard would clearly perpetuate the complexity and inconsistency that is state law which stifles the industry.

Here is a practical example. In the wake of concern over genetics—the power of genetic information and its potential for abuse—some states require that "genetic" information be segregated from the rest of the patient's medical record and subject to different standards. Under the Markey proposal, any such state laws would likely remain in effect, either by virtue of already being in existence or by virtue of being considered more protective than the federal law. As a result, health plans, hospitals and providers would have to separate out "genetic" information from the rest of the patient's medical information and treat it differently.

This raises several practical concerns. First, the states may vary in terms of what is considered "genetic." Even assuming states could agree on what they define as "genetic," as a physician, I can assure you that virtually every piece of medical information is, by its very nature, genetic. Eye color, gender, the predisposition to breast cancer are all examples of genetic information. So, how do we, as a practical matter, separate this information out from other, "non-genetic" medical information. Second, state rules regarding segregation will vary. As such, we would be potentially subject to 50 different sets of rules regarding segregation and use of this critical information. Finally, the practical implication of such limitations is devastating. The value of so-called genetic information is immeasurable and is directly responsible for the development of such breakthrough drugs as Herceptin, which provides, for the first time, real hope to women suffering from breast cancer and their families.

Rather, federal law should subject *all* patient health information, including genetic information, to the same strong standards for protection. While each of the Senate proposals would provide new federal standards for protecting all such information (albeit differently), the on-going ability of states to apply different law and the attendant lack of preemption of such state law, directly undermines this shared goal.

Thank you, Mr. Chairman, for allowing me to share with you Genentech's principles and concerns regarding patient confidentiality. The House Commerce Committee has been a vital partner in assuring a stable and fruitful environment for biomedical research, as illustrated by your recent efforts on the Food and Drug Administration Modernization Act (FDAMA). Please understand that the ultimate impact of this issue is no different, and is directly related to innovation and research.

Be assured that we share your commitment to protecting and safeguarding patient information; after all, patients ultimately are our business. Also understand, though, that information is the lifeblood of research and to the ability of the health care delivery system to enhance and assure quality. Patients are deserving of one strong law that secures all such information equally, and provides one clear set of

rules regarding how patient information must be safeguarded, how it may be used, and the penalties that will apply for any misuse.

We applaud this Subcommittee's effort and look very forward to working with you and others toward the final enactment of strong, workable and, most importantly, uniform federal standards protecting the confidentiality of patient medical information.

Mr. BURR. Thank you, Dr. Stump.

The Chair would recognize Ms. Visco at this time for an opening statement.

STATEMENT OF FRAN VISCO

Ms. VISCO. Thank you. I am here as a breast cancer survivor and the president of the National Breast Cancer Coalition, an organization that represents more than 500 member organizations from across the United States and more than 60,000 individuals.

Our focus is on eradicating breast cancer. That is our goal, our mission. Our focus is on research, making certain that there are sufficient high quality research to get the answers to this disease and also policies that will support access to care, access to quality care. And we understand that we need more information and we need research in order to determine what do we mean by quality care.

Access to care is not enough. It has to be access to quality care, and we support research that will get those answers also. But there is a problem that we are facing. And the problem is that the public has lost confidence and trust in the medical and scientific community. Perhaps when we had it; it was misplaced. But the fact is that now it is lost. The evolving health care system is—plays a major role in why we have lost that confidence, but there it is.

Patients won't go into research. It is very difficult to get them involved. We are very concerned about the use and misuse of information. Information is the lifeblood of research. It is my life and it is my blood and I have a right to make certain that it is protected and it is used appropriately.

We certainly don't want to hamper research. We don't want to erect unnecessary barriers to care. No one wants to do that. The issue is what is a necessary barrier? Losing the confidence and trust of the people who are the subject of this research is the No. 1 barrier to care—to research. That is what hampers research. That is what we need to correct.

What we want to do is create an atmosphere of collaboration and partnership where patients and the scientific community move forward together in getting the research, where we trust that the information that we have given is going to be used. And we need a minimal set of Federal standards in order to achieve that trust, to reinstate that confidence and that atmosphere which would bring us closer more rapidly to the answers that we need.

So what do we need? We need to make certain that, wherever possible, the information that is used is identified. We are looking at the explosion of technology that Mr. Markey described and that you are all aware of. We can use that explosion to help.

Perhaps there are ways we can use it creatively to keep track of individuals who have participated in research, to help get their consent. We need to have standardized consent that will make it easier for individuals to give consent. We need to make certain that

there is IRB-type review and oversight of both public and private research.

It hasn't created inappropriate barriers in public research, and we know it won't in private research always. To establish that trust once again, we have to make certain that we have anti-discrimination legislation protecting people from the abuse and misuse of their genetic information. And we need to make certain that Federal legislation and Federal regulations are a strong floor.

Once we have established the trust in the public once again, there will be less pressure on the States to establish their own regulations and their own laws. And if industry is concerned about this, they can adhere to the strong estate regulations, and they would have the uniformity that they seek.

Right now we are looking at the law in Minnesota. I think it is a wonderful example of why Federal legislation should be a floor. Here we have an evolving situation. The law has already been amended once. What we need is to use that kind of a situation to educate and inform the American public so they understand the importance of giving their consent.

They understand that the consent they give is for the use of research, the use of information and research that will be well-protected and will get the answers. If we educate the public about the importance of giving their consent, they will. They want the answers. If they trust us that we won't abuse the information that we are using, they will let us use it. They want the answers. They want us to get the answers that will further their health and the health of their families.

And finally, what we need are strong penalties. It isn't enough to have a wonderful law in place if there is absolutely no strong right to enforce your right under that law, and what we need is the right to sue.

I very much look forward on behalf of the National Breast Cancer Coalition to continuing to work with you to make certain that we have effective Federal legislation that creates a floor that we can buildupon.

Thank you.

[The prepared statement of Fran Visco follows:]

PREPARED STATEMENT OF FRAN VISCO, PRESIDENT, NATIONAL BREAST CANCER COALITION

Thank you, Mr. Chairman and members of the Committee for inviting me to testify today. I am Fran Visco, President of the National Breast Cancer Coalition and a breast cancer survivor. I am one of the 2.6 million women living with breast cancer in the U.S. today.

The National Breast Cancer Coalition (NBCC) is a grassroots advocacy organization dedicated to eradicating breast cancer. We are made up of 500 member organizations and more than 60,000 individual women, their families and friends. The NBCC seeks to increase the influence of breast cancer survivors and other activists over public policy in cancer research, clinical trials, and access to quality health care for all women.

The NBCC believes strongly that we need to establish a national policy that ensures an individual's right to privacy with respect to personally identifiable health information. We believe that our illness, diagnosis, treatment and prognosis is very personal information, whether we are breast cancer survivors, women battling breast cancer, or women with a predisposition to breast cancer. We also know that the misuse of our health information can harm us and our families. Unauthorized or inadvertent disclosure of our health status, genetic or family history can make it difficult if not impossible for some women and their daughters to obtain health

insurance. At the same time, NBBC believes that legislation protecting privacy rights should not impede the progress of biomedical, behavioral, epidemiological and health services research. Research offers women diagnosed or predisposed to breast cancer the best hope for finding a cure, improving treatment, and someday preventing breast cancer. NBCC believes that research can be carried out in a way that protects the privacy rights of individuals and simultaneously enhances public trust in medical research.

We are at a decision point where we can allow the computer revolution to make access to our personal health information a free-for-all or where we can harness the new communications technologies to insure that our personal health information remains private. Because access to health records and information is so critical to the progress of research, we may need a new paradigm to protect an individual's privacy—even if it should cost more. Research can not be held to a lower standard for protecting privacy: it must be held to a higher standard to ensure the public's support and trust.

How can we maintain the public trust? By establishing key safeguards for personally identifiable health information. By requiring informed consent and ensuring that it is not coerced. By limiting disclosure to the minimal information necessary. By establishing strong penalties for those individuals who violate these protections and by supporting the highest quality peer-reviewed research.

NBCC believes that Congress needs to provide consumers with important new rights, including:

Access to Medical Records. Individuals should have certain rights with regard to their medical record and information in order to understand how they are being used and maintained. Individuals should have reasonable access to their records to inspect, copy, supplement or amend their medical records. Individuals should also be able to seek special protection for certain sensitive information that they do not wish to be disclosed. For example, many women would not wish to disclose genetic information such as BRCA 1 and BRCA 2 test results to insurers or employers, but would want this information made available to their health care providers.

Notice of Information Policies. It is also important that individuals understand how their medical records are to be used and when and under what circumstances information will be disclosed to a third party. Plans and other health care providers should be required to notify individuals about their disclosure policies and to keep records when information is released, to whom it is provided, and for what purpose, and make that information available to individuals. Individuals should also be able to withdraw consent or limit what information is disclosed.

Informed Consent. Any legislation should strictly limit the use of identifiable health information absent an individual's informed consent except as explicitly permitted in legislation for public-interest purposes (such as public health for use in legally authorized disease and injury reporting, public surveillance or a public health investigation or intervention, health oversight, and emergency purposes). There should be clear circumstances when protected health information will not be disclosed, such as for marketing, insurance underwriting, or employment purposes without authorization of the individual. Moreover, plans, providers and others should be required to de-identify as much protected health information as possible and limit disclosure to only the information necessary for the approved purpose.

Medical Research: There has been much debate about what are appropriate safeguards for personally identifiable information with regard to research, and much discussion about whether current federal regulations can sufficiently protect patient confidentiality. Increasingly, much health services, epidemiological, biological and statistical research relies on the use of medical or health records and does not involve any interaction between the researcher and the patients. Researchers have legitimately raised serious questions about the feasibility of seeking authorization from thousands or possibly millions of individuals. Other research such as retrospective or secondary research relies on archival patient materials, including medical records and tissue specimens also does not involve interaction directly with individuals. And while the data can be encrypted, researchers and epidemiologists need to link this data back to individuals in order to generate meaningful conclusions regarding the benefits and adverse outcomes of particular treatments, as well as medical effectiveness.

The question for Congress, and for patient advocates like NBCC who care deeply about the research mission and are committed to privacy protection—is when to require voluntary informed consent to conduct research and under what circumstances to allow the disclosure of protected health information without patient authorization.

Under the common rule, research organizations conducting federally funded or regulated research projects must establish and operate institutional review boards

(IRBs), which are responsible for reviewing research protocols and for implementing federal requirements designed to ensure the safety of human subjects. No human-subjects research may be initiated, and no ongoing research may continue, in the absence of IRB approval. Integral to conducting research under the common rule is a requirement that there is proper informed consent and documentation of that consent.

There is also a mechanism under the common rule that allows for the IRB to waive the need for informed consent—but only under certain limited situations where: 1) the research involves no more than minimal risk to the subjects; 2) the waiver or alteration will not adversely affect the rights and welfare of the subjects; 3) the research could not practicably be carried out without the waiver or alteration; and 4) whenever appropriate, the subjects will be provided with additional information after participation.

Thus, IRBs currently deliberate and make decisions about when informed consent is and is not necessary. The burden is on the researcher to demonstrate to the members of the IRB why informed consent is not necessary. There should be another test for deciding on whether to waive the requirement for informed consent. The IRB should be required (in addition to the criteria above) to determine if the importance of the health research outweighs the intrusion into the privacy of the individual. In this way, the IRB would be able to successfully balance the need for the research with an individual's right to privacy.

There are two problems with the current system I would like to note: first, there are serious problems with institutional review boards; and second, not all health research is subject to IRB. Increasingly, there is health research that falls outside the common rule. This raises questions about building a new system, with an increased responsibility to protect privacy, on a flawed program.

Nevertheless, NBCC believes that IRBs are an appropriate paradigm to build upon. Before doing that, we recommend that any legislation require a serious review by the Secretary and a requirement that the Secretary make recommendations regarding standards for protecting privacy in research and improvements in the system to ensure its success in meeting its responsibility to individuals involved in research.

We also believe that Congress should extend the common rule to all research. There is always an opportunity for protected health information to be disclosed that could be harmful—even if that information is eventually aggregated. There needs to be one system for protection that applies to all research; not carve outs for this or that type of health research.

Preemption: In order for any standard to be effective it needs to be uniform across the states, but we would only support preemption if it sets a floor for the states and not a ceiling. Many states have already begun to respond to the many complex issues involved in protecting medical privacy and have established strong laws. We should not force them to a lower standard.

Penalties: Finally, we believe there should be strong criminal and civil penalties for intentionally or negligently using individually identifiable health information. Individuals should also have a civil right of action against anyone who misuses their protected health information.

One area that has been sorely absent in the debate over medical privacy is the urgent need for adopting genetic anti-discrimination legislation. Even if we pass the perfect medical privacy bill, we will not be able to entirely prevent unlawful disclosures. When privacy is breached, anti-discrimination legislation would prevent misuse of the information. These two protections go hand-in-hand. Anti-discrimination legislation in itself is hard to enforce, and therefore it is important to provide good privacy protection.

Breast cancer remains the most common form of cancer in women. We still do not know the cause or have a cure for this dreaded disease. Over the past two years, there have been incredible discoveries at a very rapid rate that offer fascinating insights into the biology of breast cancer, such as the isolation of breast cancer susceptibility genes and discoveries about the basic mechanisms of cancer cells. These discoveries have brought into sharp focus some of the areas of research that hold promise.

NBCC believes that legislation protecting medical information and privacy should be balanced. We want to see federal standards that safeguard personal health information and protect the ability of researchers to conduct vital biomedical research. We don't believe that you can have one without the other. Knowledge about how to prevent and cure breast cancer will only come if women participate in research. But without appropriate safeguards against misuse, public distrust will increase and few women will be willing to participate in research efforts, whether donating tissue or enrolling in clinical trials. Only if women believe that their individual

health information will be kept private so that it can't be used against them by insurers or employers or be made public will they have the confidence to participate in clinical research. I can't emphasize enough that we must focus our attention on building public trust. It has to be something real, something believable, if women are to place their trust in the medical and research process.

Mr. Chairman, and members of the Committee, thank you again for the opportunity to testify. We look forward to working with you on this critically important issue. I'll be happy to answer any questions you may have.

Mr. BURR. Thank you, Ms. Visco.

The Chair would take this opportunity to announce we expect a vote at any minute. There is also reason to believe that there will be at least a Republican conference that Republican members will have to leave for.

It is the Chair's intention then to put this committee in recess probably about 12:25 or 12:30 depending on when the vote is called until 1:15 to allow witnesses to have lunch and to allow that conference to take place just so you know.

STATEMENT OF DAWN M. GENCARELLI

Mr. BURR. And at this time, the Chair would recognize Ms. Gencarelli for an opening statement.

Ms. GENCARELLI. Mr. Chairman and members of the committee, thank you for the opportunity to testify before you today.

I am Dawn Gencarelli, and I am here today on behalf of Harvard Pilgrim Health Care. Harvard Pilgrim is the largest health plan in New England and has been caring for patients over 25 years. Harvard Pilgrim currently provides for 1.5 million members in Massachusetts, Rhode Island, Maine, and New Hampshire through a network that includes more than 23,000 physicians and 140 hospitals.

I am pleased to have the opportunity to testify today and would like to review the varied patient interests that must be considered in a thoughtful debate about medical record confidentiality, describe Harvard Pilgrim's efforts to reconcile these multiple interests with strong protections for the confidentiality of our members' medical information, and highlight the importance of the legitimate uses of medical information to assure the quality of care that is delivered to our members.

Harvard Pilgrim recognizes the importance of the many issues raised by medical record confidentiality and the challenges it poses for patients and health care providers during this time of rapid change in both the delivery of health care and the technology of clinical health information systems. They are complex issues that involve a careful balance to ensure that all of our patient interests are served even when they appear to conflict.

Our organization has spent an extensive amount of resources exploring our policies and practices around confidentiality. We have conducted numerous focus groups and one-on-one interviews with our members to better understand their concerns. Patients do have a right to expect that their medical information will be kept confidential as well as a strong interest in receiving high quality integrated health care.

To assure this quality of care, clinicians must have access, in a timely manner, to information pertaining to prior medical history and possible drug interactions. In addition, health plans must have access to information in order to perform functions that are de-

signed to promote quality of care including quality assurance, utilization management, disease management, case management, and peer review.

The above functions enable Harvard Pilgrim and other health plans to eliminate unnecessary variation and treatments and procedures, for example, cesarean sections; identify patients who could benefit from specialized care through one of our disease management programs; develop educational programs for our clinicians regarding specific treatments and advance technologies; and ensure that patients being released from the hospital have the appropriate support to safely return home.

In addition to receiving high quality integrated health care, patients have an interest in the advancement of research through the collection of population-based information in the protection of the public health and in having the systems of their health care organizations operate smoothly and without fraud. At Harvard Pilgrim we have worked diligently to serve the many interests of our members even when they appear to conflict.

Organizational flexibility, commitment by senior management, as well as cooperation and communication between health care providers and their patients are necessary to meet these multiple patient needs. Harvard Pilgrim has taken steps to optimize its organizational privacy protections including the removal of patient identifiers from clinical and administrative patient information whenever possible, the creation—and the creation of a safety zone to ensure to the fullest extent possible that patient information remains confidential.

This safety zone is created through the implementation of a number of policies and practices that create heightened security around medical information. Within our organization, we have established a confidentiality oversight committee that is responsible for developing and maintaining a corporate confidentiality policy. As part of this process, the committee reviews all policies and procedures throughout the organization relating to confidentiality.

In conjunction with our corporate policy, Harvard Pilgrim has developed a framework for defining appropriate uses of information by third parties as well as guidelines for the release of information. Each of these initiatives seeks to ensure that only that information which is necessary to meet an appropriate clinical or health plan need is accessed or released, that it is used by appropriate individuals for the amount of time necessary to achieve the designated purpose, that it is used within a secure environment, and that it is not subject to secondary release to unauthorized users.

Harvard Pilgrim continues to explore these and other innovative efforts in an attempt to respond to our evolving understanding of our members' needs and to continue to serve as a national leader on the issue of patient confidentiality.

As this committee contemplates the passage of legislation on this very important issue, it must ensure that the provisions of such legislation promote quality of care rather than prevent functions that support it. As illustrated by the recent enactment and subsequent suspension in Maine of a medical record confidentiality bill, good intentions can sometimes cause unintended consequences that put patients at risk.

The Maine law prevented family members from accessing information about the condition of their loved ones and medical providers from obtaining information necessary for the proper treatment of patients. To severely limit access to information will, in fact, lead to increased confidentiality but will jeopardize the other very important interests of our members.

Harvard Pilgrim has invested heavily in our efforts to ensure patient confidentiality and respects this committee's exploration of this very important issue. We must be cognizant, however, of the very real dangers that may result from poorly drafted legislation in this area including decreased quality of care, increased health care costs, an unhealthy population, and systems wrought with fraud.

Confidentiality can and must be achieved without halting appropriate and legitimate uses of information.

I thank you for your time.

[The prepared statement of Dawn M. Gencarelli follows:]

PREPARED STATEMENT OF DAWN M. GENCARELLI, HARVARD PILGRIM HEALTH CARE

INTRODUCTION

Mr. Chairman and members of the Committee, thank you for the opportunity to testify before you today. I am Dawn Gencarelli, Manager of Health Policy for Harvard Pilgrim Health Care (Harvard Pilgrim). Harvard Pilgrim is the largest health plan in New England and has been caring for patients for over 25 years. Harvard Pilgrim currently provides care to more than 1.5 million members in Massachusetts, Rhode Island, Maine, and New Hampshire through a network that includes more than 23,000 physicians and 140 hospitals.

I am pleased to have the opportunity to testify today, and would like to:

- review the varied patient interests that must be considered in a thoughtful debate about medical record confidentiality;
- describe Harvard Pilgrim's efforts to reconcile these multiple interests with strong protections for the confidentiality of our members' medical information; and
- highlight the importance of the legitimate uses of medical information to assure the quality of care that is delivered to our members.

ISSUES

Harvard Pilgrim recognizes the importance of the many issues raised by medical record confidentiality and the challenges it poses for patients and health care providers during this time of rapid change in both the delivery of health care and the technology of clinical health information systems. They are complex issues that involve a careful balance to ensure that all of our patient interests are served, even when they appear to conflict. Our organization has spent an extensive amount of resources exploring our policies and practices around patient confidentiality. We have conducted numerous focus groups and one-on-one interviews with our members to better understand their concerns.

Patients have a right to expect that their medical information will be kept confidential as well as a strong interest in receiving high quality, integrated health care. To assure this quality of care, clinicians must have access, in a timely manner, to information pertaining to prior medical history and possible drug interactions. In addition, health plans must have access to information in order to perform functions that are designed to promote quality of care, including quality assurance, utilization management, disease management, case management, and peer review.

The above functions enable Harvard Pilgrim, and other health plans, to eliminate unnecessary variation in treatments and procedures (i.e., Cesarean sections); identify patients who could benefit from specialized care through one of our disease management programs; develop educational programs for our clinicians regarding specific treatments and advanced technologies; and ensure that patients being released from the hospital have the appropriate support to safely return home. In addition to receiving high quality, integrated health care, patients have an interest in the advancement of research through the collection of population-based information, in the protection of the public health, and in having the systems of their health care

organizations operate smoothly and without fraud. At Harvard Pilgrim, we have worked diligently to serve the many interests of our members, even when they appear to conflict.

Organizational flexibility, commitment by senior management, as well as cooperation and communication between health care providers and their patients, are necessary to meet these multiple patient needs. Harvard Pilgrim has taken steps to optimize its organizational privacy protections, including the removal of patient identifiers from clinical and administrative patient information whenever possible, and the creation of a "safety zone" to ensure to the fullest extent possible that patient information remains confidential.

This safety zone is created through the implementation of a number of policies and practices that create heightened security around medical information. Within our organization, we have established a Confidentiality Oversight Committee that is responsible for developing and maintaining a corporate confidentiality policy. As part of this process, the committee reviews all policies and procedures throughout the organization relating to confidentiality. In conjunction with our corporate policy, Harvard Pilgrim has developed a framework for defining appropriate uses of information by third parties, as well as guidelines for the release of information. Each of these initiatives seeks to ensure that only that information which is necessary to meet an appropriate clinical or health plan need is accessed or released, that it is used by appropriate individuals for the amount of time necessary to achieve the designated purpose, that it is used within a secure environment, and that it is not subject to secondary release to unauthorized users. Harvard Pilgrim continues to explore these and other innovative efforts, in an attempt to respond to our evolving understanding of our members' needs and to continue to serve as a national leader on the issue of patient confidentiality.

CONCLUSION

As this Committee contemplates the passage of legislation on this very important issue, it must ensure that the provisions of such legislation promote quality of care rather than prevent functions that support it. As illustrated by the recent enactment and subsequent suspension, in Maine, of a medical record confidentiality bill, good intentions can sometimes cause unintended consequences that put patients at risk. The Maine law prevented family members from accessing information about the condition of their loved ones and medical providers from obtaining information necessary for the proper treatment of patients. To severely limit access to information will in fact lead to increased patient confidentiality, but it will jeopardize the other very important interests of our members. As an integrated system of care, Harvard Pilgrim relies on the *internal* use of information, which must be distinguished from the external disclosure of information. The internal use of information allows us to conduct essential functions, including those designed to safeguard the high quality, integrated care we deliver to our patients. In some cases, these functions are mandated by state law or by national accrediting bodies, including the National Committee for Quality Assurance (NCQA).

Harvard Pilgrim has invested heavily in our efforts to ensure patient confidentiality and respects this Committee's exploration of this very important issue. We must be cognizant, however, of the very real dangers that may result from poorly drafted legislation in this area, including decreased quality of care, increased health care costs, an unhealthy population, and systems wrought with fraud. Patient confidentiality can, and must, be achieved without halting appropriate and legitimate uses of information.

I thank you for your time.

Mr. BURR. Thank you.

The Chair at this time would recognize Ms. Abbey Meyers for purposes of an opening statement.

STATEMENT OF ABBEY MEYERS

Ms. MEYERS. Yes, thank you very much.

The National Organization for Rare Disorders represents approximately 20 million people with rare diseases who are spread all over the country. It is a total of 6,000 rare diseases, each one affecting fewer than 200,000 Americans.

Congress needs to pass a medical privacy law not only because of the Kassebaum-Kennedy law but because the European Union

requires that E.U. countries cannot trade with any country that does not adequately protect patient confidentiality. So it is very important that something is done very quickly on this issue because it is liable to turn into an international trade problem.

But also patients want and desperately need medical confidentiality on a national basis. People are not telling their doctors the truth because they are afraid that if something is written in their record, especially about a serious disease, that they will lose their insurance, their insurance price will go up, or they are going to be stigmatized in some way if somebody finds out.

So it is very important that the public is guaranteed confidentiality so that they are truthful with their physicians. This covers not only things like sexually transmitted diseases or maybe drug abuse problems but also the fact that hereditary diseases can be very stigmatizing. People are not telling their doctors that their mother or their aunt may have had breast cancer, for example, because they are afraid it will raise the cost of their health insurance.

So today the only problems—the only group of people who have problems accessing medical records are patients themselves. And this is a real problem when you walk into a doctor's office, you want copies of your own medical records. You have to sign a pile of papers that you don't understand because they are written in very legal language. Some of the waivers—actually you have to forfeit your legal rights in order to get copies of your own records.

And you sometimes have to wait weeks or months to get those records. And you find out that the hospital or the doctor can charge you. And there is no standard fee, and some doctors might charge you a dollar a page. It might turn out to cost hundreds of dollars for a copy of your own medical records. And we have heard of many cases where doctors refuse to give the patient medical records probably because they are afraid of getting sued for malpractice or some personal reason that they have, but they absolutely refuse.

Now, the problem is that there is no Federal law that requires that the identifiable medical records are kept in locked files. So very often when you walk through your doctor's office, you find somebody else's file laying there, and you can read it. There is nothing to stop you from reading it.

Insurers can obtain information about our health that has nothing to do with the bills they are paying. They can find out the entire record of your mental health treatment when they look through your files to pay for the bills for a broken leg. Local pharmacies are releasing our prescription data to pharmaceutical companies with no regulation at all. And once somebody knows what drugs you are taking, they know what is wrong with you.

All confidential information can be sent, and it is, to a huge computer up in Massachusetts called the Medical Information Bureau. George Orwell could not have invented a better model of the intrusive Big Brother. It contains your medical information and mine—millions and millions of Americans. Anything that you thought could be kept secret in your doctor's office is on a computer in Massachusetts that any insurance company in this country can access.

Clerks right out of high school can get into it and find out what your medical information is. So we must have confidentiality assur-

ances. We must have an absolute minimum floor that says no State can legislate less, but States will be allowed to legislate more.

Thank you.

[The prepared statement of Abbey Meyers follows:]

PREPARED STATEMENT OF ABBEY MEYERS, PRESIDENT, NATIONAL ORGANIZATION FOR RARE DISORDERS

Mr. Chairman, members of the Committee, thank you for inviting me to testify before you today on behalf of patients with serious and chronic diseases. I am Abbey Meyers, President of the National Organization for Rare Disorders (NORD), which represents people with over 6,000 rare "orphan diseases." Each rare disease affects fewer than 200,000 Americans, but combined together they all affect an estimated 20 million Americans. Most rare diseases are genetic, and the need for medical privacy profoundly affects not only those who have hereditary diseases but also every member of their extended family.

Today even "healthy" people are learning that they are affected by privacy issues because, as the Human Genome Project is discovering, virtually every human being carries genetic abnormalities that will eventually impact our lives or the lives of our children. NORD is also an active member of the Consumer Coalition for Health Privacy, which includes a broad range of consumer, patient, disability, and professional groups committed to the development and enactment of public policies and private standards that guarantee the confidentiality of personal health information and promote both access to high quality care and the continued viability of medical research.

Besides the obvious need for Congress to enact federal legislation governing medical privacy—the August 21 deadline and the European Union's privacy regulation that may diminish trade with the United States if privacy guarantees are not firmly set in place—American consumers are clearly demanding that Congress enacts federal privacy guarantees that require an individual's consent before our personal medical information is released to anyone.

The current lack of a federal law safeguarding the privacy of medical records significantly diminishes access to and quality of health care in the U.S. Out of fear that disclosure of their medical records may result in denial of insurance, loss of employment or housing, and stigmatization and embarrassment, many people withhold information from their doctors or simply avoid seeking care. In fact, a survey released by the California Health Care Foundation in January found that one in five Americans believes their health information has been used or disclosed inappropriately and one in six engages in some form of "privacy-protective" behavior when they seek, receive or pay for health care. As a result, they risk inadequate care or undetected and untreated health conditions.

People are being forced to choose between their privacy and receiving health care. In addition, important public health activities, such as outcomes research, quality initiatives and population-based studies, are compromised by incomplete or inaccurate data.

PATIENT ACCESS TO MEDICAL RECORDS

The ironic fact is, under our current patchwork system of privacy, the only people who have trouble accessing their medical records are consumers themselves. If you want copies of your own medical records, you generally have to sign a myriad of legal papers (some of which are hardly understandable to the ordinary person), you may have to sign waivers forfeiting your legal rights, you usually have to wait days or weeks to obtain the copies, and your physician's office or hospital can charge you a fee for every piece of paper you request.

While consumers across the country face extraordinary problems accessing their own medical records, pharmaceutical companies can easily obtain sensitive information from local pharmacies revealing the names of drugs that have been prescribed to you, your neighbor may read your entire medical history in your doctor's office because your case file is not kept in a locked cabinet, your insurance company can read your confidential psychiatric record even though they may be investigating billing for your broken leg, and they can send all of this information to the huge Medical Information Bureau (MIB) in Massachusetts so that clerks at all insurance companies (not just your own insurer) will be able to investigate your medical history any time they want to.

REAL-LIFE EXAMPLES

Examples of abuses of medical information are all too common and troubling.

- Just last month, Aetna health insurance claims forms blew out of a truck en route to a recycling center and scattered on I-84 in East Hartford during rush hour. Aetna quickly dispatched employees to scoop up the forms, which contained identifiable personal health information. Under company policy, these papers should have been shredded, but were not.
- In another troubling example, the Harvard Community Health Plan, a Boston-based HMO, admitted to maintaining detailed notes of psychotherapy sessions in computer records accessible by all clinical employees. Following a series of press reports, the HMO revamped its computer security practices.
- In a more personal case, a woman who was hurt in an auto accident found that the defendant's lawyer subpoenaed her medical records and announced in court that when she was 16 years old this woman had a baby outside of marriage and gave it up for adoption. There is no reason that an attorney in a automobile accident case should have had access to the woman's gynecological records!

The victims of these privacy violations ranged from large groups to a single individual and the causes ranged from negligence to bad practices. While no federal law can prevent all future abuses, the enactment of a strong, comprehensive law with meaningful enforcement will help to create a regulatory and legal framework that will require the holders of identifiable health information to protect health information and appropriately limit its use or risk significant penalties.

CONSUMER RIGHTS

Obviously, insurance companies need access to medical information for treatment and payment purposes, and scientific researchers require access to medical records. But, consumers should give their consent before anyone is allowed to access our records, even insurance companies. For example, some people do not want their insurance company to know that they took a genetic test, so they pay for the test themselves. If the doctor writes in the patients record that the test was positive for a hereditary disease, the insurance company should not be privy to information that the insurance company did not pay for. These companies should only gain access to information that is directly relevant to the product or service they are paying for.

Let me explain that the "consumers" I am talking about in these examples represent two distinct classes of people:

One class of consumers are generally healthy people who may see a doctor irregularly for common maladies such as colds or flu, and who may sometimes take pharmaceuticals for occasional fever, colds or pain. These people expect the government to protect them, for example, by assuring through regulation that treatments are effective and have minimal risk. They cannot imagine that strangers would want to see their medical records, they have no idea how many people have access to this sensitive information, and it does not occur to them that there may be a commercial value for the sale of private medical information to others. Nevertheless, these "healthy" people may have had a grandparent who died of Alzheimer's disease, an uncle with schizophrenia or epilepsy, or a parent who had breast or prostate cancer, and they may not want their next door neighbor to be privy to this information nor their employer, nor even their spouse or children. There can be medical information that a person will share only with their physician. Without a firm guarantee of confidentiality, people are unable to talk honestly and openly with their doctors.

The other class of "consumers" is composed of sick people: Usually those with serious or chronic illness who see doctors on a regular basis because of a health problem. These people may be willing to take greater risks in order to identify more effective treatments, or to locate superior medical services that might extend their life or improve their quality of life. Many of these individuals are willing to participate in medical research, and thus they may be willing to endure a lesser degree of medical privacy as long as they can maintain control over who will be privy to their medical records. If they do not want researchers, hospitals, drug companies, etc., to pry into their medical records, they want the option of refusing access to this information.

RESEARCH

Fortunately, people who participate in federally funded research, or research that will be used in an application for FDA approval, must sign an "informed consent" document approved by an Institutional Review Board (IRB), and they can choose not to participate if they feel their privacy will be violated.

Certainly one of the most challenging debates now before you is how to address privacy concerns related to privately funded research that is not being conducted in anticipation of FDA review and therefore not required to gain IRB approval. We know that Congress has been examining this problem for some time, and we consumers are very aware that you are trying to find a solution. .As an advocate for people with serious and chronic illness let me make clear that we believe that scientific research is extraordinarily important, and you must find a way to protect consumer's medical information without hampering the progress of medical research.

The best way to accomplish these goals is to expand the IRB and informed consent process to all research, regardless of funding source. Through the informed consent process, people who participate in research are told how many parties will have access to their records, and they are assured that the treating institution will not allow access by unauthorized personnel. In those cases where the informed consent process is excessively burdensome and the threat of a privacy breach to the individual is minimal, the IRB can waive the informed consent process.

The problem now is that these rules apply only to research involving federal funds or application to the FDA. The rules must be applied all research no matter what the funding source. The ethical obligations that researchers have to their subjects, and the individual's right to appropriate informed consent, do not change depending on the funding stream.

It is also important to note that some "medical" research is actually "marketing" research, and Congress must clearly define parameters that protect consumers from unwanted intrusions of their privacy by those who will not actually enhance scientific knowledge. In most cases, simply making case records anonymous by replacing a person's name with a code number, will solve the problem.

PREEMPTION OF STATE LAW

In the absence of federal protections, the states have acted to varying degrees to create protections for their residents and one of the major questions before the Congress is how the federal law will interact with these state laws. Will the federal law be the "ceiling" above which states are forbidden to act, or a "floor" above which states can enact stronger laws.

Let me say clearly that this is a critical question for people with rare diseases because clinical research on orphan diseases is usually conducted at numerous sites in various states, primarily because there are not often enough patients in any one state available for study. Therefore, it is crucial that federal government enact a "floor" that guarantees all Americans, regardless of their state of residence, a set of minimum protections. At the same time, as people with serious and chronic illnesses, we believe that states must maintain their right to enact stricter privacy laws to address the specific needs of their residents. If local laws become too strict, certainly local residents and lobbyists will point the flaws out to local policymakers.

In other words, the federal government, by enacting a national medical privacy law, will set absolute minimum standards that all states must obey. Such a minimum will create broad uniformity across the country, preempting the vast majority of state laws, which are weaker than the federal proposals. Any state, however, that wants stricter privacy laws should be allowed to enact and enforce them.

In addition, we firmly believe there are at least two areas of medical information that deserve special protections: 1) genetic information, and 2) psychiatric records. Several states have already enacted laws to protect these very sensitive areas and more states should be encouraged to do so. Mental health treatment notes are particularly sensitive. Insurance companies used to ask therapists for summarized notes and treatment plans. But in the last few years they are asking for complete copies of patient records that reveal the most sensitive private information that should never leave a therapists office.

Mr. Chairman, the esteemed members of this committee should understand that at this very moment your personal medical records may be known to people in this room. They may know the medicines you take and the diseases you are being treated for, as well as your spouse and your children. Certainly you can remember a few years ago when a Vice Presidential candidate had to withdraw his name because his psychiatric record was made public (Senator Eagleton). Only a few years ago Senator Pryor's medical record was made public when he had a heart attack. There may be people in this very Congress who have a stigmatizing psychiatric diagnosis, or a history of a sexually transmitted disease that you caught at the age of 18, or a predisposition to a genetic disease that, if known, could put your next election at risk. These facts ought not to become public record. In the absence of a federal

"floor" for medical privacy, there is nothing to prevent the wrong people from using your medical history for the wrong purposes.

No one should have access to your medical information or mine without our knowledge and consent. This is what consumers want and need. We urge you to do so quickly.

Mr. BURR. Thank you, Ms. Meyers.

The Chair would recognize, for purposes of an opening statement, Mr. Krinsky.

STATEMENT OF DANIEL L. KRINSKY

Mr. KRINSKY. Mr. Chairman, Congressman Brown, members of the subcommittee, the National Association of Chain Drugstores appreciates the opportunity to present testimony today regarding the important issue of protecting the confidentiality of patient medical records in today's modern health care delivery system.

My name is Daniel Krinsky. I am a registered pharmacist. I am the director of patient care services and pharmacy practices at Ritzman Pharmacies in Wadsworth, Ohio. Ritzman Pharmacies is a small family owned eight store chain located just outside of Akron, Ohio. We specialize in a wide range of innovative and advanced pharmacy services including diabetes management, home infusion, and hypertension management.

Let me begin by stating that NACDS supports enactment of a strong confidentially law that will preempt the patchwork of existing State laws and protect patient privacy. We want our patients to have confidence that their personal information is secure while allowing chain pharmacies to appropriately utilize medical information as health care providers to maintain and improve patient care.

NACDS has worked for years to take a leading role on protecting patient privacy. Attachment one to my statement are "Ten Principles To Protect The Confidentiality Of Consumer Medical Records" that our industry created and continually updates to ensure chain pharmacies operate with protecting patient privacy as a top priority.

To mention some of the key pharmacy confidentiality legislative issues—because retail pharmacies process about 50 percent of all health care payment claims, it is important that new Federal requirements for patient confidentiality not have a disproportionate effect on the ability of retail pharmacies to operate efficiently or provide integrated comprehensive patient-oriented prescription services.

NACDS supports Federal standardization of patient confidentiality safeguards that includes:

First, Federal preemption of State laws. There are approximately 31,000 chain community pharmacies many of which operate across State lines. However, more and more States have been enacting their own new and differing privacy laws and regulations making it increasingly difficult for multistate pharmacies to understand and comply with these laws in an efficient manner. Adding another Federal law on top of this or trying to determine which law is stronger as some bills call for would create even more challenges.

Second, NACDS supports the use of a single consolidated authorization for the purpose of obtaining patient authorization to use and disclose patient information for payment, treatment, and health care operations. Such authorization is provided at the time

that the patient enrolls in a health plan or when an uninsured patient provides an authorization for these purposes to an originating provider of a prescription. Under this approach, the patient's prescription will be sufficient to use patient information for the purpose of practicing pharmacy as defined in State practice laws and by regulatory boards. This approach also limits the recordkeeping and recording burdens of the patient or the provider.

Since up to 40 percent of patients have others pick up or deliver both new and refill prescriptions, obtaining the additional separate authorization from all patients would be next to impossible. Imposing a requirement that the patient personally pick up a prescription would inconvenience the patient and could jeopardize the health of the elderly, children, or the infirm who can't otherwise physically get to the drugstore.

In 1990, Congress passed the Omnibus Budget Reconciliation Act, OBRA 90, which recognized that delivering pharmacy service involves more than just filling an original prescription. The role of the pharmacist, which continues to evolve, includes enhancing outcomes for medication use. In part, as a result, pharmacy providers now engage in a wide range of activities that use patient information. These include refill reminder programs, prospective and retrospective drug use review, disease management, physician-pharmacy collaborative practice agreements, and formulary management.

The definitions of health care and treatment of any confidentiality legislation should include compliance programs, refill reminder programs, and pharmacy programs recognized by Federal and State agencies as disease management programs. Any Federal confidentiality law must recognize and provide flexibility for the evolving role of community pharmacy in the health care system. Most recently, the Health Care Financing Administration issued regulations reimbursing diabetes education management programs and pharmacies and many States recognize the value of pharmacy professionals providing educational and counseling services.

Some legislative proposals will require pharmacies to maintain records for 7 years and document each and every case in which patient information was disclosed to create an audit trail, such as the date, purpose, and description of information disclosure even when patient information is used for treatment or obtaining payment.

Such a proposal would result in enormous if not impossible workload requirements on our pharmacists and disclosure records would number in the multiple billions. The benefit of an audit trail and how often it is used must be weighed against the increased cost to the health care delivery system.

Patient care must not be compromised in the name of added paperwork. Consumer costs must not be driven up by excessive regulation and basic common sense protections for privacy must take precedence. Let me reiterate that the use of electronic records and technology, if carefully coordinated and protected, results in a much safer and secure system that protects patient confidentiality while providing for optimum care.

In conclusion, we applaud you for holding this hearing on this complex but critical issue. With my testimony, I have also attached a list of key implementation issues and questions for persons to

think about while drafting provisions with a potential impact on pharmacy.

Thank you for providing me with this opportunity to testify today on behalf of Ritzman Pharmacies and NACDS.

[The prepared statement of Daniel L. Krinsky follows:]

PREPARED STATEMENT OF DANIEL L. KRINSKY, DIRECTOR, PATIENT SERVICES AND PHARMACY PRACTICE, RITZMAN PHARMACIES, INC., ON BEHALF OF NATIONAL ASSOCIATION OF CHAIN DRUG STORES

Mr. Chairman and Members of the Subcommittee, The National Association of Chain Drug Stores (NACDS) appreciates the opportunity to present testimony today regarding the important issue of protecting the confidentiality of patient medical records in today's modern health care delivery system.

Founded in 1933 and based in Alexandria, Virginia, the NACDS membership consists of over 130 retail chain community pharmacy companies. Collectively, chain community pharmacy comprises the largest component of pharmacy practice with over 93,000 pharmacists. The chain community pharmacy industry is comprised of over 19,000 traditional chain drug stores, 7,000 supermarket pharmacies and nearly 5,000 mass merchant pharmacies. NACDS members operate more than 31,000 retail community pharmacies with annual sales totaling over $135 billion including prescription drugs, over-the-counter (OTC) medications and health and beauty aids (HBA). Chain operated community retail pharmacies fill over 60% of the more than 2.73 billion prescriptions dispensed annually in the United States. Additionally, NACDS membership includes more than 1,400 suppliers of goods and services to chain community pharmacies and 96 international members from 26 foreign countries.

Executive Summary: NACDS Supports a Strong National Law

Let me begin by stating that NACDS supports enactment of a strong Federal confidentiality law that will preempt the patchwork of existing state laws and protect patient privacy. We want our patients to have confidence that their personal information is secure, while allowing chain pharmacies to appropriately utilize medical information as health care providers to maintain and improve patient care.

On this note, I'd like to point out that NACDS has endorsed S. 881, "*The Medical Information Protection Act of 1999*," introduced by Senator Robert Bennett (R-UT). Senator Bennett has been working to perfect his legislation for over five years and the resulting "Bennett bill" is the most comprehensive and thoughtful medical records privacy legislation introduced in Congress to date. While the legislation rightfully imposes tough penalties for the misuse of confidential patient information, it is carefully balanced to allow providers sufficient flexibility to appropriately utilize patient information to optimize patient care. It would also protect patient data without the inconvenience of burdensome paperwork on patients and providers.

NACDS also has worked for years to take a leading role on protecting patient privacy. Attached to my statement are ten "*Principles to Protect the Confidentiality of Consumer Medical Records*" that our industry created and continually updates to ensure chain pharmacies operate with protecting patient privacy as a top priority.

Key Pharmacy Confidentiality Legislative Issues

Because retail pharmacies process about fifty percent of all health care payment claims, it is important that new Federal requirements for patient confidentiality not have a disproportionate effect on the ability of retail pharmacies to operate efficiently or provide integrated, comprehensive patient-oriented prescription services. NACDS supports Federal standardization of patient confidentiality safeguards that includes:

Federal Preemption of State Laws: There are approximately 31,000 chain community pharmacies, many of which operate across state lines. However, more and more states have been enacting their own new (and differing) privacy laws and regulations, making it increasingly difficult for multi-state pharmacies to understand and comply with these laws in an efficient manner. Adding another Federal law on top of this or trying to determine which law is stronger, as some bills calls for, would create even more challenges for multi-state pharmacy operations.

Conflicts between Federal and state law could be virtually impossible for health care providers to identify and resolve on a patient-specific basis. Moreover, does the law in the state in which the patient resides prevail, or does the law in the state in which the product or service is being provided govern the transaction? This question is particularly important for pharmacies located near state borders.

Without Federal preemption, patients will be required to wait longer to obtain their prescription medications because pharmacies will be required to take additional time to determine whether to follow a specific provision of state or Federal law. For each patient, the pharmacist must first identify any conflicts between provisions of Federal and state law and then compare those provisions to determine which is the most restrictive. The pharmacist must make these two legal decisions while patients, or their designees, are waiting for their medications.

Making legal decisions is a job for attorneys, NOT for health care providers who are trying to provide medication as efficiently and expeditiously as possible to sick patients. The impact on our patients is our most paramount concern, and, therefore, NACDS supports a comprehensive Federal standard that preempts state confidentiality laws.

A Single Consolidated Authorization for the Use and Disclosure of Personally Identifiable Health Information (PHI): NACDS supports the use of a single consolidated authorization for the purpose of obtaining patient authorization to use and disclose PHI for payment, treatment and health care operations. Such authorization is provided at the time that the patient enrolls in a health plan, or when an uninsured patient provides an authorization for these purposes to an "originating provider" of a prescription. Under this approach, the patient's prescription will be sufficient to use PHI for the purpose of practicing pharmacy as defined in state practice laws and by regulatory boards. This approach also limits the recordkeeping and reporting burdens of the patient or the provider.

To maximize patient convenience, any Federal confidentiality law must require employers, health plans, and originating providers to obtain from the patient a *single consolidated authorization* to use and disclose that patient's personally identifiable health care information for the purposes of treatment, payment, and health care operations.

Down-stream health care providers MUST be able to legally assume that the single consolidated authorization has been obtained, otherwise these providers will be forced to require patients to take the time to fill out an additional separate authorization form to protect themselves from litigation alleging a breach of the patient's confidentiality.

Since up to 40% of patients have others pick up or deliver both new and refill prescriptions, obtaining the additional separate authorization from all patients would be next to impossible. Imposing a requirement that the patient personally pick up a prescription would inconvenience the patient and could jeopardize the health of the elderly, children, or the infirm who can't otherwise physically get to the drug store. Under some legislation already introduced, prescriptions could not be refilled until patients have signed the necessary multi-point authorization form, causing yet another patient inconvenience.

Recognition of Pharmacy Practice Activities as a "Continuum of Care": In 1990, Congress passed the Omnibus Budget Reconciliation Act (OBRA 90), which recognized that delivering pharmacy services involves more than just filling an original prescription. The role of the pharmacist, which continues to evolve, includes enhancing outcomes from medication use. Pharmacy providers engage in a wide range of activities that use PHI. These include refill reminder programs, prospective and retrospective drug use review, disease management, physician-pharmacy collaborative practice agreements, and formulary management.

Moreover, given that over 70 percent of all prescriptions are "managed" by pharmacy providers for PBMs and third party payors, pharmacies are often contractually obligated to provide some of these services, to a range private and public plans, including Medicare+Choice plans, Medicaid and some Federal Employee Health Benefit (FEHBP) plans. NACDS believes that any new Federal law should recognize that pharmacy is an evolving health profession whose role is to enhance appropriate outcomes from medication use through a continuum of care approach.

The definitions of health care and treatment in any confidentiality legislation should include compliance programs, refill reminder programs and pharmacy programs recognized by Federal and state agencies as disease management programs. Any Federal confidentiality law must recognize and provide flexibility for the evolving role of community pharmacy in the health care system. Most recently, the Health Care Financing Administration issued regulations reimbursing diabetes education management programs in pharmacies and many states recognize the value of pharmacy professionals providing educational and counseling services.

Implementation Issues for Retail Pharmacies

There are several important issues for chain community pharmacy relating to the implementation of new Federal privacy laws. Some of the more important considerations include:

Originating Providers: NACDS supports the rights of patients to inspect, copy and amend their medical records, and that the originating provider is the appropriate place for these operations to occur. Originating providers are those that initially prescribe a course of treatment and create the historical medical record, such as health plans, physicians or emergency rooms.

The originating provider of the prescription must be the primary source for patients to access, copy, and amend their health care information.

Audit Trail Related to Disclosures: Some proposals would require pharmacies to maintain records for seven years and document each and every case in which PHI was disclosed—such as the date, purpose, and description of information disclosure—even when PHI is used for treatment or obtaining payment.

Such requirements would create tremendous time and work burdens on pharmacy providers, given that PHI is used for multiple operations each day to assure that the patient receives the appropriate therapy, the pharmacy meets operational guidelines of third party payors, and the pharmacy is reimbursed for providing the service. Such a proposal would result in enormous if not impossible workload requirements on our pharmacists and disclosure records would number in the multiple billions. The benefit of an audit trail and how often it is used must be weighed against the increased costs to the health care delivery system.

Sufficient Time to Modify Computer Systems: Like most health care providers, chain pharmacies have invested in expensive and sophisticated computer software systems to help process claims and help deliver pharmacy services. NACDS believes that a realistic time frame is needed to implement new uniform confidentiality standards, including time to develop software and hardware, test and distribute new products, and train employees in their use. Retail pharmacy estimates a minimum of 18 months would be needed to implement a new confidentiality law, once a law is passed or regulations are finalized.

Use of NCPDP Standards: The entire pharmaceutical industry relies on the National Council for Prescription Drug Programs (NCPDP) to establish standards for electronic transmission of prescription payment claims. Any new Federal confidentiality law must recognize the important role that NCPDP has and should continue to have as a standard-setting organization for the billions of retail pharmacy payment claims.

Other Key Issues

Other issues not specific to pharmacies are also extremely important to the entire health care continuum. Expanding or creating new Federal regulatory oversight of health provider operations must be examined carefully. Patient care must not be compromised in the name of added paperwork; consumer costs must not be driven up by excessive regulation; and basic common sense protections for privacy must take precedence.

For instance, creating an entire new right of private action specific to privacy should not be necessary. Consumers currently have legal recourse to sue if their medical records are used inappropriately.

In addition, especially when it comes to prescription drugs, falsely obtaining a prescription drug or controlled substance without a valid script from a physician can result in severe penalties and prosecution under Federal and state law. The penalties included in legislation introduced to date are severe, and would certainly deter any effort by a business or entity to illegally use or disclose patient identifiable information.

Let me reiterate that the use of electronic records and technology, if carefully coordinated and protected, results in a much safer and secure system that protects patient confidentiality, while providing for optimum care. Avoiding millions of pieces of paperwork that must be filed and maintained increases the protection of health care records.

Because this issue is so complex and so dependent upon the use of technology, detailed attention must be given to the coordination of technology and health care systems. It is critical that legislators and regulators "get it right." As was seen earlier this year in the state of Maine, a law that may sound good to consumers, but is not perfected before implementation, can disrupt the entire health care system. The Maine law was suspended by the legislature after being in effect for just two weeks and is currently under a two-year review.

In conclusion, we applaud you for holding this hearing on this complex but critical issue. With my testimony, I have also attached a list of key implementation issues and questions for persons to think about when drafting provisions with a potential impact on pharmacy. Thank you for providing me with the opportunity to testify today on behalf of Ritzman Pharmacies and NACDS. I'll be glad to answer any questions you may have.

ATTACHMENT 1

NACDS PRINCIPLES TO PROTECT THE CONFIDENTIALITY OF CONSUMER MEDICAL RECORDS

1) **Patients Have the Right to Know Who May Access, Use, Share, or Further Disclose, Patient Identifiable Health Care Information.** Insured patients' informed consent must be in writing, signed, and obtained by either the employer or the health plan. Uninsured patients' informed consent must be in writing, signed, and obtained by the originating provider who prescribes or orders the health care services.

2) **A Patient's Informed Consent Should Authorize** . . . health care providers to access, use, and share or further disclose patient identifiable health care information, to: 1) Provide treatment; 2) Seek payment; 3) Manage programs which improve outcomes and health care quality or result in reduced costs to consumers; and, 4) Undertake health care operations and utilize sufficient administrative information to support all of the above.

3) **One National Law** . . . must be the product of a national debate to assure confidentiality of patient medical records, while at the same time promoting quality of care and not unnecessarily increasing health care costs. It will be much easier for both patient and health care provider to understand and comply with one national law rather than 51 laws . . . a national law plus 50 different state laws.

4) **Employers Must be Prohibited from Accessing Patient Identifiable Health Care Information** . . . unless the patient signs a separate informed consent form.

5) **Non-Patient Care or Marketing Activities** . . . must be authorized by a separate patient consent for programs that are outside of the scope of treatment, payment, management of programs which improve outcomes and health care quality or result in reduced costs to consumers, and health care operations/administrative information.

6) **"Treatment" . . . is defined as everything that state boards of pharmacy allow pharmacists to do within the definition of the practice of pharmacy, including compliance, disease management, outcomes, and other quality assurance programs, from which patients may freely choose to withdraw or opt-out.**

7) **Patients Must have the Right to Inspect, Copy, and Amend (but not change) their Medical Records** . . . at the originating provider, for a fee to cover copying and administrative costs.

8) **Computer Security Must** . . . safeguard patient identifiable health care information that is maintained or transmitted for any purpose.

9) **The National Law Must Go into Effect Within a Reasonable Timeframe** . . . to provide patient confidentiality protection as soon as possible, but also to allow health care providers reasonable time to develop, test, distribute, and to be trained to use new software to help them comply with this lengthy and complex legislation.

10) **Those With Legitimate Access to Patient Identifiable Data Must Commit to Maintain and Abide by Confidentiality Laws.** Penalties and fines should be imposed if individuals or entities knowingly and intentionally break the law.

ATTACHMENT 2

KEY PHARMACY ISSUES WITH MEDICAL RECORDS CONFIDENTIALITY LEGISLATION

May 27, 1999

Key Issues

- Full Federal preemption of the patchwork of state privacy laws, with an allowance for exceptions for communicable disease reporting, essential health data and vital statistics collection, is critical. Precedent exists in the financial institution sector. Without Federal preemption . . . pharmacies and pharmacists will NOT be able to comply with laws that cannot be readily found or quickly compared for conflicts between Federal and state law.
- Written authorizations should be obtained by originating providers, such as health plans and physicians, but not be required for downstream treatment authorized by those providers. Pharmacies account for about 50% of all consumer health care payment claims and patients and pharmacies could not handle additional form requirements for each prescription or initial visit.

- Consolidated authorizations for treatment and payment must create a "legal presumption" that allows pharmacies and other downstream health care providers to rely upon: that individuals, presenting health insurance cards or a valid prescription, have provided the necessary authorization for treatment and payment from their employer or health plan. **The same assumption must be recognized for the non-insured . . . the originating provider obtained the necessary authorization.**
- The definition of health care or treatment should include pharmacy compliance and disease management programs that are often required by Federal laws and rules and are a continuation of dispensing the prescription.
- Electronic data collection and data transmission provisions dealing with payment must not limit our ability to perform drug utilization review (DUR) and other quality enhancement measures, often required by Federal and state law.
- Pharmacists should not be required to obtain authorizations for counseling patients on OTC drugs.
- The definition of "individual representative" or next of kin should not interfere in allowing family members, friends, caregivers or neighbors to pick up prescriptions for patients.
- Pharmacy benefit cards must NOT be included in payment and electronic payment transaction limitations. If so, pharmacies which would no longer be allowed to transmit the NCPDP payment claim for payment because its information is MUCH broader than that required for payment. As a result, pharmacy benefit managers and health plans would no longer have access to the clinical information contained on the NCPDP payment claim necessary for DUR.
- Assurances should be made that Federal agencies will not use new penalty authority as they have under the False Claims Act or Controlled Substance Act to pursue providers for innocent and technical errors. If there is no harm to the patient and mistakes are innocent, providers should not be unduly punished for employee error.

Key Questions in Drafting Confidentiality Legislation

- Does the definition of health care include over-the-counter (OTC) drugs and medically "related items"? It should not, as the workload, confusion and consumer inconvenience would be prohibitive.
- Will bill language interfere in the common tradition of allowing relatives, friends, caregivers and neighbors pick up prescriptions for patients?
- Is it the intent of legislation to require separate, written authorizations for each pharmacy customer, despite the fact that patients have their choice in deciding where to deliver prescriptions to pharmacists directly, asking for treatment and granting permission for pharmacists to dispense and be paid?
- Have members and staff contemplated the impact of "Administrative Billing Information" and payment provisions and their possible impact on the use of the NCPDP prescription payment claim forms and PBM clinical data collection used for utilization review?
- Is it clear that pharmacy benefit cards are not considered a "payment card"?
- Do lawmakers know that software experts have told industry that 18 months is the minimum time needed to create, test, and train pharmacists in using new software for pharmacy compliance with a new Federal privacy law and that it is unlikely that software can be developed and implemented for a bill that does not substantially preempt state laws?
- Is it the intent of legislators to limit the use of prescription information to issue discount coupons for over-the-counter drugs and products related to the treatment or prescription by requiring a written authorization?

Mr. BURR. Thank you, Mr. Krinsky.

The Chair would recognize for purposes of an opening statement Mr. Latanich.

STATEMENT OF TERRY S. LATANICH

Mr. LATANICH. Thank you, Mr. Chairman.

I have been watching to see if I was going to be the last witness on this panel or the first half of the recess, but I guess I will go last.

My name is Terry Latanich. I want to thank you, Mr. Chairman, and members of the subcommittee. I am senior vice president of

Merck-Medco Managed Care which is a subsidiary of Merck. We do manage the prescription drug benefit for more than 1,100 health plans and cover more than 50 million people.

The patients that we serve, as well as the plant sponsors, count on us to protect the patient's health and their confidential medical information. We take both of these responsibilities very seriously. I would like to begin today by giving you one real-world example of how we use patient identifiable information.

A member of one of the health plans that we serve was taking a medication for an enlarged prostate. Later, this patient was prescribed medicine to treat depression. Unfortunately, the use of that anti-depressant not only worsened the patient's prostate problem, it can also result in serious problems for elderly patients like fractures.

We were able to use this patience's prescription history to identify this potential health problem. Our pharmacist contacted the physician who had prescribed the anti-depressant. The physician was not aware that the patient had a prostate problem or that he was taking medications for it. Once informed, the physician changed the patient to an anti-depressant that was safe for the patient and didn't exacerbate the prostate problem.

This interaction was identified by a program which we call Partners for Healthy Aging. Merck-Medco processes more than 300 million drug claims a year and maintains a point-of-sale data base that includes about a billion claims. But the use of this data set demonstrates the power of the ability to protect patient health and safety.

Last year two drugs were voluntarily withdrawn from the market. Posicor, a drug used to treat hypertension and angina, and Duract which is used to manage acute pain. Studies showed that Posicor had potentially serious interactions with nearly two dozen commonly used drugs. Duract was withdrawn because its use may have resulted in up to four deaths and the need for several liver transplants.

Many physician's offices lack the computer systems to readily identify patients using a specific drug. Merck-Medco's immediate access for our patients' specific data base enabled us to take immediate action. On the day that each product was withdrawn from market, we stopped dispensing those drugs in our pharmacies and alerted our retail pharmacy networks that no further prescriptions of the recalled drugs should be filled.

Within days of the withdrawals, we sent out over 81,000 letters to physicians who had prescribed Posicor or Duract to the members of any health plan that we serve. These letters identified patients under their care who had received a prescription for the recalled drugs. In addition, we sent more than 233,000 letters to patients using these medications and encouraged them to contact their doctor.

One of the emerging capabilities of prescription drug management is improving the health of patients with chronic diseases through patient and physician education. As indicated by the earlier witness, we also provide programs here such as diabetes, MS, asthma and cardiovascular disease.

We also use patient information to communicate with physicians best medical practice guidelines. Studies indicate that compliance with just one of these practice guidelines in the area of cardiovascular disease reduces mortality by 30 percent and morbidity by 50 percent. Yet this practice standard is followed less than 50 percent of the time.

Medco identifies patients through our data base who are potential candidates for modification therapy based on these medical practice guidelines. We inform the prescribing physician of the practice guideline, see if the physician wants to alter the regimen to comply with that best practice guideline, and then give the opportunity for the physician to make that decision.

Such use of patient identifiable information allows for dramatic improvement in health and safety. We take seriously our responsibility to protect patient medical information. We use advanced security systems on our data bases to ensure that patients inside or outside the company do not have access to patient identifiable information unless authorized and that authorization is strictly limited to those with a need to know.

Merck-Medco does not provide patient-identifiable information to any marketing firm, any drug manufacturer, or even our parent, Merck and Company. Let me emphasize this again. No identifiable information is given to anyone for marketing purposes. We view this being consistent with our role as a health care provider and our professional standards of ethics.

While we believe that our stand is sufficient to provide medical record confidentiality, we do support the enactment of legislation in this area. Our hope is that any legislation will meet three tests.

First, it should not create any impediments to the kind of activities which I just discussed and which clearly improve patient health and safety.

Second, it is imperative that any provisions that require patients to authorize the use of this information provide for consolidated authorization. As an organization, to provide services to health plans, we need to be able to rely on the plan sponsor's enrollment of a member as evidence that disclosure has been made and consent has been obtained. It would be very difficult for us to collect individual consent forms for these services. We would have to obtain more than 50 million consents annually and maybe even more under some legislative proposal.

Finally, we strongly encourage the development of a uniform Federal standard for medical record confidentiality that will set the bar high enough to provide the requisite level of protection. Without such a uniform national standard, we will face the daunting challenge of determining which State law to apply.

If I could just close with one example of the difficulty that we face operating in 50 States, it may resonate with you. A patient may live in one State, work in another, they may receive Medicare and use pharmacies in both States. The plan they use may be located in yet another State. The patient may see a physician or pharmacist in another State on vacation and the records of the health plan may be maintained in the data base located in another.

With legislators considering a staggering number of medical record confidentiality bills, we face the practical problem of how

you maintain confidential against a patchwork of legislation. We would submit that a floor is very difficult for a provider to deal with on a real world day-to-day basis. In trying to understand which State's law to apply where there may be conflicts is very, very difficult.

There are opportunities to look to see whether there can be secretarial discretion so we do not have to deal with the problem of not having the bar high enough.

We would encourage you to adopt the uniform standard and have it be preemptive across the States.

[The prepared statement of Terry S. Latanich follows:]

PREPARED STATEMENT OF TERRY S. LATANICH, SENIOR VICE PRESIDENT, MERCK-MEDCO MANAGED CARE, L.L.C.

Good morning Mr. Chairman and members of the subcommittee. My name is Terry S. Latanich and I am Senior Vice President for Government Affairs for Merck-Medco Managed Care, LLC, a subsidiary of Merck & Co., Inc. I am responsible for directing Merck-Medco's federal legislative and regulatory programs, including developing our legislative policy on medical record confidentiality. In addition, however, I have significant business responsibilities including overall management responsibility for our largest client, the Blue Cross and Blue Shield Federal Employee Program which covers nearly 5 million individuals. In my testimony today I would like to focus on five issues:

1. The roles and responsibilities of managers of the pharmacy benefit;
2. The importance of developing, maintaining, and using large computerized medical record databases to protect health and safety;
3. The importance of using both patient-specific and encrypted data to manage the health status or disease states of persons using prescription drugs;
4. The importance of having a statutory authorization or consolidated consent to enable those who manage the benefit plans to effectively, and efficiently, administer prescription drug benefits; and
5. The need for a uniform national standard for medical records confidentiality.

BACKGROUND ON MERCK-MEDCO

Merck-Medco has been managing prescription drug benefits since 1982, initially as a public company called Medco Containment Services, Inc., which was acquired by Merck & Co., Inc., in 1993. Merck-Medco manages the prescription drug benefit for more than 50 million Americans. Our customer base includes (1) more than 50 percent of the Fortune 500 companies; (2) more than 20 Blue Cross and Blue Shield plans; (3) more than 60 percent of the lives covered in the Federal Employee Health Benefit Program (including the plans offered by BCBS, GEHA, APWU and SAMBA); (4) several state employee/retiree programs including CALPERS and all or part of the state employee/retiree programs in Ohio, Texas, Massachusetts, Louisiana, and Georgia; and (5) several union sponsored health plans.

Merck-Medco provides prescription drug care primarily through operating subsidiaries. The first, PAID Prescriptions, processes more than 270 million drug claims annually from 55,000 retail pharmacies nationwide. To do this, Merck-Medco operates a highly sophisticated point-of-sale ("POS") claims system that verifies eligibility and drug coverage, checks for drug interactions, and informs the retail pharmacy of the amount it should collect as the copayment from a member of a health plan to which we provide service. Merck-Medco's POS system takes less than one second to process each claim once we receive it from a retail pharmacy. Three years of history are maintained in Merck-Medco's POS system, creating a database of nearly one billion claims.

Merck-Medco's other subsidiaries, the Merck-Medco Rx Services pharmacy companies, constitute the largest mail service pharmacy organization in the world. We fill more than 50 million prescriptions annually through 12 pharmacies located in eight states. Each of these pharmacies uses the most sophisticated dispensing technology available. The combination of high technology and strong pharmacist involvement in the dispensing process allows Merck-Medco to be very cost effective while maintaining the highest dispensing accuracy rates in all of pharmacy. Merck-Medco employs more than 11,000 employees including 1,700 pharmacists. Merck-Medco also operates two licensed pharmacies that do not dispense drugs; but that are dedicated

to counseling patients and physicians on appropriate prescribing and prescription drug use.

1. The Role and Responsibilities of Pharmacy Benefit Managers

Merck-Medco is sometimes referred to as a "PBM" or "Pharmacy Benefit Manager". But there are a variety of organizations that provide "PBM services" by internal management including a number of HMOs (e.g., Kaiser Permanente), integrated health systems, hospitals, some Blue Cross and Blue Shield plans, and a number of insurance carriers. Whether a sponsor offering a prescription drug benefit decides to "build or buy" pharmacy benefit manager capabilities, the principal services required to manage the prescription drug benefit include:

- Processing prescription drug claims through sophisticated, real-time point-of-sale computer systems that adjudicate claims in a matter of seconds
- Negotiating provider contracts with retail pharmacies, including performance standards and reimbursement schedules, to provide services to members of health plans
- Providing a mail service pharmacy option through which members can fill prescriptions for medications, generally involving chronic conditions
- Reviewing the drugs that have been prescribed, at the point-of-sale, before those prescriptions are dispensed, to minimize the potential for adverse or dangerous drug/drug interactions or other potentially life-threatening problems
- Creating procedures to review drugs that may (i) be appropriate for some, but not all, members, (ii) require special management due to especially high costs or (iii) require controls because they are susceptible to abuse
- Managing drug utilization by reviewing patterns of the use of prescription drugs (e.g., by reviewing the claims database it can be determined whether a patient is consistently late refilling prescriptions for chronic illnesses which suggests that the patient is not taking the medication as prescribed (e.g., skipping days or taking the drug at wrong dosages)
- Managing patients' health by using prescription drug history to identify persons with specific diseases and offering them programs and/or information to improve their health status
- Managing the cost of a health plan's prescription drug program by working with the health plan to develop strategies for negotiating pricing concessions from pharmaceutical manufacturers through the use of formularies or similar strategies.

2. Maintaining and Using Large Computerized Databases

Patient-identifiable data is critical to the services provided by Merck-Medco, whether for purposes of processing claims, auditing for fraud and abuse, verifying prescriptions, checking for drug interactions or dispensing prescriptions. Our data inputs are three-fold:

- Plan sponsor provided information such as eligibility files and in some instances medical claims;
- Patient supplied information including prescriptions, self-reported information from patient profile forms, and information submitted by the patient in health or disease management programs; and
- Physician supplied information including prescription information and diagnoses and related information necessary to conduct health and disease management programs.

As I noted earlier in my testimony Merck-Medco manages a database of nearly one billion drug claims. It is our experience that confidentiality can be maintained in such systems. At Merck-Medco access to this database is limited to those with a "need-to-know." We employ state-of-the-art security systems for ensuring that persons inside or outside the company do not have access to patient-identifiable information unless specifically authorized. Most views of the data are on a blinded basis (e.g., epidemiological research). Systems capabilities are continuously improved, for example, improving the ability to track and audit any instance in which a patient record has been viewed.

Merck-Medco does not provide patient-identifiable information to any marketing firm or drug manufacturer, including our parent Merck & Co. We do, however, use aggregated, non-identifiable data for a variety of purposes. Encrypted or blinded data has many important uses, such as epidemiology, outcomes research and health economics.

An example of how our use of data is protecting patient safety was the 1998 market withdrawal of two prescription medications due to serious and even potentially fatal adverse drug reactions. Merck-Medco immediately implemented safety measures to prevent dispensing of Posicor®, a drug used for hypertension and angina,

when it was voluntarily recalled by Roche Laboratories on June 8th, and when Duract®, a nonsteroidal anti-inflammatory (NSAID) used for short-term treatment of acute pain was pulled by Wyeth-Ayerst Laboratories on June 22nd. The voluntary withdrawal by Roche of Posicor was due to the possible dangerous interactions with two dozen other widely used medications. Duract was withdrawn from the market because of several reports of deaths or liver transplants required because of liver function problems associated with the drug.

On the day the drugs were withdrawn from the market, Merck-Medco took several steps to prevent possible harm or death to the beneficiaries of our health plan clients. Physicians often do not have the office-based computer systems to readily identify patients using a specific medicine. Identifying patients at risk involves a slow and inefficient process of manually reviewing each patient's medical record in the doctor's office. Merck-Medco's immediate access to patient-specific data enabled it to take swift and decisive action to address this situation. On the day each product was withdrawn from the market Merck-Medco suspended dispensing of all prescriptions for Posicor and Duract in its mail service pharmacies. Merck-Medco also sent electronic messages to all 55,000 pharmacies in its PAID Prescriptions pharmacy network advising them of the market withdrawals and recommending that no further prescriptions of the recalled drugs be dispensed.

Within days of the withdrawals Merck-Medco sent letters to the prescribing physicians for patients prescribed Posicor or Duract reimbursed under a Merck-Medco managed prescription benefit plan. Each physician letter was accompanied by a customized list of current or past patients under their care who had received a prescription for the recalled drugs to assist them in checking on those patients. Merck-Medco sent over 233,000 letters to patients and 81,000 letters to physicians during these two product withdrawals.

Using Patient-Identifiable Medical Records in Disease Management Programs

One of the emerging benefits offered by health plans are programs to help manage the progression of disease states through patient and physician education. Merck-Medco provides a number of these programs in areas such as diabetes, multiple sclerosis, asthma, and cardiovascular disease. Merck-Medco can improve patient self-management of these conditions through the patients' participation in such programs. We identify patients who could potentially benefit from such programs by analyzing their existing prescription drug records. In other cases, patient-identifiable data are used in communicating with physicians treating the patient enrolled in one of these programs to encourage compliance with "best medical practice standards."

For example, the best medical practice guidelines as outlined in the 1997, Vol. 336, New England Journal of Medicine article by Magnus Johannesson states that a certain type of cholesterol reducing drug, an HMG (e.g., Lipitor®, Mevacor®, Pravachol® or Zocor®) should be started post myocardial infarction. Studies indicate that compliance with this protocol reduces mortality by 30 percent and morbidity by nearly 50 percent. Yet, this practice standard is followed less than 50 percent of the time. Through Merck-Medco's health management program for congestive heart failure, we are able to identify those patients who are potential candidates for this modification in therapy, contact the prescribing physician, inform the physician of the practice guideline, and see if the physician wishes to modify the prescribed drug regimen. The use of patient-identifiable information and a sophisticated database allows for this dramatic improvement in patient health and safety.

Another compelling example of the need to continue to allow for the use of patient-identifiable information in the management of prescription drug benefits is found in Merck-Medco's Partners for Healthy Aging® program which is designed to improve appropriate prescribing and prescription drug usage among the elderly. At the core of the Partners for Healthy Aging program are a series of drug utilization review rules that protect seniors from drugs and dosages that are inappropriate given their age. For example, the use by the elderly of long-acting benzodiazapines such as Valium® or Librium® can result in dizziness, loss of balance and increased risk of hip fracture. Other drugs require dosage reductions in the elderly. Merck-Medco's Partners for Health Aging program is succeeding in improving health outcomes because of our ability to combine and analyze patient-specific information from prescription information and self-reported profile data from patients and to communicate what we know from this analysis to patients and their physicians. I have attached to my testimony a copy of the recent JAMA article describing the outcomes of this program. Nearly 25 percent of the time a physician was contacted through the program, the physician either modified the prescription previously written or discontinued the drug.

4. The importance of a Consolidated or Statutory Authorization

One of the key issues that Congress must consider in developing legislative standards for maintaining the confidentiality of patient identifiable medical information is whether and how to implement an authorization process for the use and disclosure of such data—separate from the consent to be treated by a health care provider or separate from the enrollment by an individual in a health plan.

Ideally, Congress could draft a law that statutorily sets out and defines certain circumstances or specific purposes or activities for which identifiable patient information could be used or disclosed without an individual's consent. For example, Congress could create a "statutory" authorization for health plans and providers to use an individual's identifiable health information for purposes of treatment, payment and specified "health care operations" once that individual has enrolled in the health plan or consented to be treated by the health care provider.

Some have argued that separate, discrete authorizations should be obtained from individuals each and every time that their health care information is accessed. Such a multiple authorization scheme would unnecessarily interfere with, or even shut down, the ability to provide quality, cost-effective health care.

While the statutory authorization approach may be preferable, from our viewpoint, it may not be achievable. An alternative approach embraced by a number of existing proposals involves the concept of a "consolidated authorization". We think that the ability to obtain a single, consolidated authorization from an individual upon enrollment in a health plan or when consenting to treatment by a health care provider that authorizes the use of the individual's information for purposes of providing treatment, securing payment for that treatment and conducting health care operations of the plan or provider is crucial. It is essential, from our perspective, that Congress recognizes the need to use a "consolidated" authorization for the use of patient-identifiable information.

Merck-Medco is an organization that provides services as an agent to a health plan. We are not a stranger to the patients in these plans, but a critical part of the continuum of their care. It is imperative that we be able to rely on the plan sponsor's enrollment of a member into its health plan as evidence that disclosure of the possible uses of patient-identifiable information has been made and consent obtained. It would be extremely burdensome, perhaps impossible, for a PBM to collect individual consent forms for the services we provide. In the case of Merck-Medco, we would have to obtain 50 million consent forms annually, more often under some legislative proposals under consideration. In the context of electronically adjudicating a prescription drug transaction in under one-second we must be able to look to the patient's enrollment in a health plan as evidence of their authorization to use and disclose their personally identifiable health information for treatment, payment and their plan's health care operations activities. As a downstream provider of treatment, payment and health care operations to a health plan, we would then have assurance that the uses of patient-identifiable information we have described above fall squarely within the requirements imposed under any legislation adopted. Today, Merck-Medco and other PBMs rely on the health plan to provide us with a list of persons eligible to use the prescription drug benefit. The integrity of that eligibility transfer must be maintained.

5. Creating a Federal Standard—the need for Preemption of State laws

Merck-Medco operates in a "real-time" electronic environment with nearly one million transactions being adjudicated daily. Each year our customer service representatives and pharmacists handle in-bound or place out-bound calls to physicians and their patients across the country more than 25 million times. Our pharmacies receive prescription from patients in every state, and we receive refill orders by telephone, IVRU, fax, and Internet. Absent the adoption of a uniform national standard for the protection of medical records, companies such as Merck-Medco will face the daunting challenge of determining which state's law to apply to any given circumstance. This problem is growing daily as state legislatures consider a staggering number of medical record confidentiality bills. Enrollees in health plans often obtain medical services or prescription drugs from multiple providers in many states. Consider, for example, the situation that may be faced by a Member of Congress.

The Member may:

- Have a permanent residence in his or her home state;
- Live in Virginia while Congress is in session;
- Use a hospital in Maryland;
- Fill prescriptions in DC, Virginia and Maryland
- Travel to other states while on vacation, during which time prescriptions may need to be filled or refilled;

- Have a son or daughter attending college in a state other than the Member's home state; and
- Fill his or her maintenance medications through a mail service pharmacy in yet another state.

What state law would control the prescription drug records in this hypothetical? How should inconsistencies in state laws be resolved? Which state's law should be considered "primary" in the case of conflict? We strongly encourage the development of federal standard of medical record confidentiality that will set the bar high enough that its uniform application in all jurisdictions will provide the requisite level of protection for personally identifiable health information.

Thank you Mr. Chairman and Members of the Subcommittee for the opportunity to appear before you today. I would be happy to answer any questions you may have.

Mr. BURR. Thank you, Mr. Latanich.

The Chair at this time would ask unanimous consent to enter into the record a February 18, 1998, Washington Post editorial and a February 19, 1998, correction. The editorial suggests that CVS had arranged to supply the names of their pharmacy customers to drug companies similar to what you said, Ms. Meyers, in 1998. The Post went on to add a correction, that CVS sent data to a marketing company to track, but that the company was under contract not to release the personal data to drug companies or to others. So the Post certainly clarified their editorial based upon what the record was. Without objection that would be entered into the record.

[The information referred to follows:]

WHEN PRIVATE MEANS PRIVATE

[Washington Post, February 18, 1998]

Does the average person mind when, after having a prescription filled at the pharmacist, he or she starts getting related junk mail from drug companies to which the pharmacy has passed along his or her name, address and medical condition? Are such customers likely to be pleased at the convenience—as the pioneers of this new form of medical marketing insist they ought to be—or are they likelier to bristle at the implied violation of their privacy? Anyone who finds this a difficult question ought to glean a big, broad hint at the answer from the fierce consumer reaction to a report in this newspaper Sunday that several large area pharmacies, including those at the Giant Food Inc. and CVS chains, have entered into such arrangements with a Massachusetts-based company called Elensys. Today, in full-page ads and other formats, Giant announces it will stop providing such information—reacting to what spokespeople said had been a flood of calls from angry consumers.

And what were pharmacists—next door to doctors in their access to privileged, personal knowledge about people's ailments—doing marketing such information in the first place? The answer casts some light on the strange tensions being set up everywhere by the financial possibilities—one might better call them temptations—of the so-called "information economy," in which information about one's customers and their needs had become a vast new resource to be mined. It shouldn't surprise anyone that consumers feel more strongly about their medical prescriptions than they do about the great amounts of other information now routinely collected from every financial transaction, whether it's traveling, shopping or browsing the Internet. But information about people's preferences—meaning the sorts of things they are likely to do, or read or buy—is by far the most valuable of the various sorts of information now being briskly harvested and traded on all sides. Any company that collects such information in the ordinary course of business is sitting on a gold mine—and can be expected to act on that fact in the absence of specific, spelled-out public limits.

To what extent should people's needs be allowed to be treated this way, as some sort of naturally occurring resource available to anyone who can grab it? The outcry over drug prescriptions suggests one such limit. While some forms of sensitive information, such as credit information, are now protected, the sheer variety of types of medical data have made progress slow on protecting them.

Prescription information falls near the line between purely medical data and commercial information, but as the reaction makes clear, that line has been crossed. Besides being inherently more sensitive and personal then information about shopping

choices, prescriptions are also in a real sense less optional: Nobody "chooses" to have a particular ailment or to release the information about that ailment into the wider data stream of junk mail. The arrangements with Elensys, which contracts to manage pharmacists' data about patients and to make selected bits of it available so drug companies can send potential patients "educational material" about their inferred ailments, are just ingenious enough to focus people's attention on where they want that line drawn.

CORRECTION DATE: February 19, 1998

An editorial yesterday incorrectly stated that several large pharmacies, including Giant and CVS, passed along to drug companies the names of persons having prescriptions filled at the pharmacy. In fact, Giant and CVS sent data to a marketing company to track and write to pharmacy customers who had not re-filled prescriptions, but that company was under contract not to release the personal data to drug companies or others.

Mr. BURR. For the purposes of our witnesses at this time, we will recess, hopefully, for 35 minutes; and we will reconvene this hearing at 1:15.

[Brief recess.]

Mr. BURR. The Chair would call the hearing back to session. I hope everybody had an opportunity to get enough to eat. The Chair would recognize himself for the purposes of questions for 5 minutes.

Let me ask you, Mr. Jacobsen, could you tell me what happened in Minnesota and specifically at Mayo with the new law as it might or might not have affected pediatric research?

Mr. JACOBSEN. Pediatric research?

Mr. BURR. Pediatric research is a tough one to get people to commit to allow to happen anyway.

Mr. JACOBSEN. Right. I am trying to think back to information that we have got on that. I don't have that on the top of my head.

We did look at a study of those that gave us authorization to use the medical records versus those that didn't, but restricted that to ages 20 and older in that study. Obviously, I can't tell you what has happened with response rates for pediatrics.

Mr. BURR. Let me ask you because I have got the Bowman Grey School of Medicine, part Wake Forest University, in my district. What would researchers there be subject to if the Minnesota law were adopted in North Carolina?

Mr. JACOBSEN. It was really quite a bit of work to try to implement this. For those of you that don't know what this law was, it required us to ask all patients seen after January 1997 for a general authorization to use the medical record for research purposes.

As originally written, the default was set to no. We had to get an explicit yes. That was the amendment alluded to earlier so that the default was set to yes with reasonable contact. The systems to put that into place with close to 300,000 patient visits per year were really quite substantial. Systems to try to contact patients before they came in for their scheduled visits, to try to capture them at the time when they enter the system, which you can imagine the many different portals for entry, urgent care, emergency care, X-rays, all sorts of places. To try to catch patients that didn't have patient registrations ahead of time was really quite a task to put this altogether.

Mr. BURR. You alluded to a study that you had done. Can you tell us about the specifics of the findings of that study?

Mr. JACOBSEN. Sure. What we did was we selected a sample of patients who had been seen in the previous 3 years at Mayo and went through the same procedures that were being used clinically to comply with the law and asked them about their preferences for authorization.

We had three written contacts. What we found overall about 3 percent of people explicitly refused. About 80 percent explicitly gave us that authorization, but 17 percent didn't express their wishes at all despite three written contacts asking them for their wishes and explaining to them what would happen if they didn't give it to us.

I alluded to the findings in my testimony that there were some subject patients where their refusal rates were quite a bit higher. It all sort of makes sense intuitively in terms of younger persons, persons with conditions that some might consider sensitive, and so on. I think one of the most important things was looking at what happened with those people, that large number of people that didn't express their wishes despite asking them. I think that it is very important to keep in mind that we have got to make sure that defaults to a yes with reasonable contact with whatever legislation we have.

Mr. BURR. Let me go to Ms. Gencarelli. You stated in your testimony that the Maine law prevented family members from accessing information about the condition of their loved ones and medical providers from obtaining information necessary for the proper treatment of patients.

What happened to the Maine law?

Ms. GENCARELLI. The Maine law contained extensive provisions and requirements that required written disclosure for basically any and all release of information. Clearly it was not intended in the bill, but that was the ultimate consequence, was that it was written in such a way that authorization was required in so many circumstances that the things such as delivering flowers, administering last rites, even notifying family members of a loved one's condition were prohibited by the law and that law was sequentially suspended. And they are currently redrafting and cleaning up that law.

Mr. BURR. How fast did they suspend that law?

Ms. GENCARELLI. I believe 2 weeks.

Mr. BURR. Mr. Stump, let me ask you.

I worked closely on the pharmaceutical and biologics portion of the FDA Modernization Act. One of my goals was to streamline that approval process from the 12 to 15 years that it took to bring patients a particular treatment.

I am curious what would happen to the drug development process if archival research had conditions that—for those patients who were no longer with us that it was left up to their estates to access for permission to use that archival research?

What would it do?

Mr. STUMP. The ramifications would be substantive and significant. We are obligated to do outcome research on our products at the time they are approved. We don't have the answer to every interesting question at the time of approval.

We need to do continuing surveillance in order to ascertain how our product is doing once it goes into the general prescribing population. In order to access that data, we need a pretty efficient and streamlined process. We will do that. We have to do that. If that process becomes so cumbersome that resources have to be diverted to that process, which we would do, the costs will be products like Herceptin, that development was long and hard.

My colleague on the panel, Fran Visco, was of immense help to us in getting the patient community to even make it happen. It is that kind of high risk, high impact, meet the critical need project we're talking about. The project could have easily been sacrificed at various points along the way had we been diverting resources away from that into more complex archival studies.

Mr. BURR. Thank you.

My time has expired. The Chair would recognize Mr. Waxman.

Mr. WAXMAN. Thank you, Mr. Chairman. I thank Mr. Brown for allowing me to start my questions first because I have another hearing to attend.

Dr. Stump, let me ask you this. There is a common rule and it requires informed consent, an IRB review for practically all research conducted in this country including federally funded research and almost all research conducted at universities, major hospitals, and academic centers, and then there are similar rules when working with the FDA approvals.

You object to applying the common rule requirement of informed consent to records-based research. I hope that you are aware that the common rule specifically provides for the waiver of consent, waivers permitted when the research presents, quote, no more than minimum risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.

How do you justify treating your records-based research differently from all such research sponsored today by the Federal Government or conducted at institutions like UCLA or Harvard?

Mr. STUMP. I guess it is a question of how much time, energy, and resources you spend overseeing what is minimally risky investigation. I am not aware of abuse of that process. These IRBs do perform a critical function. We use them just like any publicly sponsored research does as well under oversight from the FDA. I want IRBs to be paying very close attention to that work and protecting patients from the near-term risk of being exposed to uncertainties in their products. I would rather not have them spending their time and energy where there is really minimal risk.

Mr. WAXMAN. Well, if you think that IRBs have done a good job and you welcome them, the IRBs are under the common rule where we have supervision over the information disclosures, and the common rule also explicitly grants expedited IRB review for records-based research.

You claim that even expedited IRB review would add unnecessary Federal oversight to some mysterious unquantified, unidentified body of research. I want to figure out exactly your concerns. If Genentech conducts records-based research to support a new drug application, it would be subject to the FDA's equivalent of the common rule; isn't that correct?

Mr. STUMP. It would be in that situation.

Mr. WAXMAN. UCLA has multiple-project assurance with the Federal Government. If Genentech sponsors records-based research at UCLA, it has got to be subjected to the common rule; right?

Mr. STUMP. In that situation, yes.

Mr. WAXMAN. So much of the research you conduct or sponsor is already subjected to what you call unnecessary Federal oversight. I think you are vastly exaggerating the impact of common rule scrutiny on the remainder of whatever research you conduct or sponsor.

That is my view. I would like to hear you respond to it.

Mr. STUMP. I guess that I would agree with you on the preapproval research. Actually, the vast majority of outcome research, so-called archival research, is done post-approval.

It is done in product surveillance. It is done in establishing the outcome experience of your product after approval by the FDA as it should have been predicted by your approval clinical trial base. That is actually where the vast majority of information is collected.

We have tracked most of our products. As one example, our heart attack drug, Activase, we track about 100,000 patients a year prospectively to determine whether that drug is working successfully, which is save lives for heart attack patients that we showed in early clinical trials. We show that very well. If every IRB at every site that provides this anonymous information had to go through the approval process, it would add an additional significant burden.

Mr. WAXMAN. It would if you did it under every single case. But if you do it under those circumstances where you are already involved in research where there is a Federal involvement, either FDA or research involving some other university, what proportion of the research conducted or sponsored by Genentech is records-based or not currently subject to the common rule?

Mr. STUMP. I don't have the fact right at hand. I could get that and provide it to you. I could tell you along the size of patient data bases that we collect——

Mr. WAXMAN. Why don't you get it for the record. Do you conduct any human subject research which is not regulated under the common rule? By human subject research, I mean research involving patients?

Mr. STUMP. We do no research for preapproval clinical trials that is not covered by the common rule.

Mr. WAXMAN. Dr. Amdur, how do you respond to what Dr. Stump is saying? Is this going to be unnecessary burdensome regulation?

Mr. AMDUR. I think this is one of those nice situations where everybody can be happy because I think that Dr. Stump's concerns about the things that he does not want to be subject to burdensome regulations, regardless of how minimal that burden is, indeed under the current common rule regulations would not be burdened.

The types of activities that he is speaking of, in my opinion as an IRB chair, are not research. We can review the regulatory definition of research. I have it here if you would like me to explain my answer, but these are things that are not being done with the goal of producing scientific generalizable knowledge. They are being done for product evaluation and marketing information. And

in my opinion, that does not satisfy the definition of research. It is certainly not a scientific study that any of us normally think of.

And the intent of the regulations was not to go around and meddle in areas that do not have to do with specific and traditional focus of research. So I think that an IRB is inappropriately misusing its authority to try and get Dr. Stump and his company to go through their system, and I don't think that that will happen to any large degree.

Mr. WAXMAN. Maybe we need to clarify these issues because it sounds like concerns that Dr. Stump is raising are concerns that you think are really not valid if we draft this thing appropriately.

Mr. AMDUR. Absolutely. To answer the second part of that, this issue of archival data on people who are deceased and going to their estates, as a question was raised, the regulations specifically define a human subject to be a living individual. And so archival research on people who are deceased is outside the authority of the Federal regulations, and companies and investigators do not have to worry about any kind of regulatory burden.

However, as you have mentioned in your response, the burden is extremely small because expedited review is a one page electronic mail application that is reviewed in real time. It is a minimal burden.

Mr. WAXMAN. Thank you, Mr. Chairman.

Mr. BURR. The gentleman's time has expired.

Could I just ask Dr. Stump for a clarification for all of the members? I think I heard you say that if we do this wrong, we will adversely affect the post-approval review of pharmaceuticals that enter the marketplace? Did I hear that correctly?

Mr. STUMP. That is not exactly what I intended if that is how it came across. I think that we will continue to do what we need to do to monitor what our products are doing post-approval.

Mr. BURR. Will it alter your access and ability to do that?

Mr. STUMP. We will figure out a way to do it. What it will alter is our ability to maintain those early stage products that are a higher risk who must be resourced from the same pool that have much longer term benefits to the general public health. We will be missing on the treatments for stroke and heart attack and cancer that are in our pipeline now at an early stage, but would be therapies 5 to 10 years from now.

Mr. BURR. The Chair would recognize the ranking member, Mr. Brown.

Mr. BROWN. Thank you, Mr. Chairman. First of all, Mr. Krinsky, thank you for joining us. I don't have a question for you, one more statement, but your comments about family, friends, designated care givers, making sure they could pick up medication at Ritzman or any other pharmacy is especially important. I think that any legislation that we draft will make sure that is protected.

Mr. Latanich, your comments I appreciate on the disease-management programs. Again, any legislation that we come up with as it goes through this process we will make sure that this actually has the authority to allow that. I think that is especially important.

Ms. Meyers, a question for you, if I could. The patients that you represent very clearly had the most to gain from medical research, yet you say they support the toughest form of Federal medical

records privacy legislation because of the nature of disorders, the consequent difficulty of attracting research dollars to them.

It seems you, perhaps among all of the witnesses, would seem to be the most interested in making sure there were no disincentives erected by us or anybody, disincentives to do the kind of research that many people need. Expand, if you would, on understanding that, on making sure that strong patient—explain how strong patient protections are especially necessary to cultivate and protect a robust research environment, if you will.

Ms. MEYERS. Research under the common rule gives consumers much more protection than they get when they go to their private doctor's office. The federally funded research and research leading to an FDA approval for a drug give privacy guarantees. When you sign an informed consent document, it tells you who is going to have access to your medical records, it will be the FDA, it will be the drug company, et cetera. It gives you a guarantee that the university or the hospital will, in some way, keep your record confidential and if papers are published, your name will not be identifiable.

And so you have wonderful guarantees that don't exist outside of the medical research arena where they are doing clinical trials on something. There are specific areas in private research that it doesn't cover. For example, in vitro fertilization is not covered by any Federal regulation and organ transplantation. So there are a number of areas where it should apply.

What we are saying to Congress basically is that consumers who aren't in research want the same protections that subjects get when they go into research. They want the benefit of signing an informed consent document that will tell them who has access to their medical record.

And if they want to refuse, they can refuse to sign it and refuse to be a subject in that trial.

Mr. BROWN. Dr. Amdur, one of the concerns raised today from—let me just—background reading on this from panelists talking today is that anything that creates any administrative burden may delay or inhibit the conduct of research. Run through for us how much work is involved in getting IRB approval for medical records research?

Mr. AMDUR. Okay. First, if I could just as background address something that I see as a systemic issue in all of these questions or many of these discussions, which is the issue of do we have a large body of privately funded research currently that is going on outside the Federal regulations? Meaning, that if you pass legislation that requires these administrative issues that you are asking about, will that create a change compared to what is going on now.

The answer is there won't be a big change because medical research in this country, by and large today, is being done for FDA application or at institutions that have already committed in writing to conducting research regardless of funding source according to Federal regulations. So enacting legislation for medical records privacy in general may very well change a lot of things compared to how they are done now, but for research—for the most part research is being done with medical records or otherwise according to the Federal regulations. So there wouldn't be a big increase in burden compared to what it is now.

What is the burden now? To get to your specific question. The burden according to Federal regulations, if you will, is stratified by risk, the potential risk to the subjects. If there is no more than minimal risk and the data is already existing, it has been collected for other reasons and there are no identifiers, it doesn't even have to go through the IRB system.

However, most research that we are discussing with medical records and that we see in this country has identifiers. And the regulations say that if you can put protections in place, encryptions, that kind of thing, locked file boxes that decrease the risk of a problem from a breach in confidentiality to no more than minimal risk from this study, then it could be dealt with by expedited review.

It is a minimal administrative burden for an investigator to obtain expedited approval for their research. At our institution it is a one page application and can be handled by electronic mail. It is reviewed by one member of the IRB or a small subcommittee rather than a full committee meeting. So it is done real time. You have a study. You call on the phone. You put a paragraph together, send it in. The next day you have approval. So it is a very low burden thing.

Mr. BROWN. Thank you. Let me shift, Ms. Visco, to you. You talked a lot about public and private, privately—publicly and privately funded research and your assertion that research should be, whether it is public or private, be held to the same standards for ensuring protection of patient confidentiality.

Do women who participate in breast cancer clinical trials, are they generally aware of the different standards for public and privately funded?

Is that even an issue that is raised in their mind?

Ms. VISCO. No, I don't think so as all. It is one of the things that we are trying to educate our constituency about, but it is not something that an individual patient who walks into her doctor's office and her doctor is knowledgeable enough to talk to her about clinical trials. No, I don't think that the question is ever asked.

Mr. BROWN. The physician would be unlikely to raise it, and the patient would be equally unlikely to inquire whether it is public or private?

Ms. VISCO. Yes, that is absolutely true. I think the system that we are talking about putting into place is not expanding the existing IRB system. There are many problems with the IRB system that we are all aware of and there are many people working on correcting those.

What we would like to see is an IRB-type system so that we don't have to—we are not asking that the Minnesota law become Federal legislation. We are asking for an oversight, a threshold that everyone has to walk through to determine whether face-to-face informed consent is appropriate in each instance.

That is what we are asking for, that threshold. We are not saying that you need to have that informed consent on a one-on-one basis in every instance.

Mr. BROWN. Okay. Thank you.

Thank you, Mr. Chairman.

Mr. BURR. Dr. Amdur, let me come back to you because I need a clarification. Under the current law, you are not required to get consent for deceased records, correct?

Mr. AMDUR. Correct, although it is not a law.

Mr. BURR. Per regulations, excuse me. There are proposals out there to expand that authority to include the need to get consent for those archival records.

Would that present a problem if that were proposed and adopted?

Mr. AMDUR. Yes, I believe that it would. Let me say that there are certain very select situations where doing research on a deceased person's information has direct implications and is linked in an intimate way to living people, such as very specific genetic research or sexually transmitted disease research.

I have never seen one of these proposals, but the point is I could imagine a situation where we could say that the research regulations indeed apply even though the subject is archival information, meaning specimens, for example, of dead people, because the very unusual nature of it directly links it to a living person with implications with identifying information.

That is a theoretical problem. I just want to record that issue. But for the types of research that are going on today, the answer is that the current regulations do not cover them, and I think that it would be an unnecessary burden and an expansion of regulatory authority to a lot of different areas that really don't need that type of protection.

Mr. BURR. I hope all of you realize the difficulty that I think most of the members are having at distinguishing a lot of different proposals that are out there and the technical nature and all of a sudden you cross the line and it does cause a problem, stay on this side of the line and it doesn't cause a problem, understanding what different recommendations are being made for person-to-person approval and that type of thing.

I want to come back to you, Dr. Stump. I want to go back to the question that I asked you, and I will ask it in a different way. If we did the wrong thing, could this committee possibly have Sidney Wolf in here telling us because we wrote it this way, drug companies and possibly the FDA and the post-approval review that goes on, that we limited the amount of information that you could accumulate on the effects of a drug that had just been approved and that was adverse to the health——

Mr. STUMP. What Mr. Wolf regularly refers to is detecting these previously unknown types of adverse events beyond the life of approval. When this happens, it is the rare event. That doesn't mean that it is not a severe event, it is just rather a event. Your chance of detecting that is directly related to the amount of information you can recover and analyze and the time with which you can do it.

Anything that delays that time or constrains your ability to expand that data base will delay your ability to detect their——

Mr. BURR. There are things that we could do that would, in fact, hurt the availability——

Mr. STUMP. Yes. The process needs to be simple, and it needs to be uniform.

Mr. BROWN. Will the gentleman yield?

Mr. BURR. I would be happy to.

Mr. BROWN. There is information on the other end. There is something on the other end we could do which would cause information to be disseminated that violated a patient's rights that might cost her a job or cost him health insurance.

So we obviously have to walk a pretty fine line; correct?

Mr. STUMP. We fully agree. There has to be accountability and those who handle this information, ourselves included, need to be held accountable through existing law. We take that very seriously.

What we are asking though is find a way to do that to protect us. All of us are patients, protect us now, but not at the needless expense of real potential long-term benefits.

Mr. BURR. I think Dr. Hamburg covered that as well with the need for there to be uniformity in what we do.

The Chair would take this opportunity to thank all witnesses and also to this panel of so many, that the lack of member participation is not an indication of lack of interest of this issue or the understanding of the seriousness of this issue.

It is more an indication of the schedule today and some significant mark ups that are taking place in this building to the significance that members on both sides of the aisle are not able to go from the first floor to the third floor in fear of the vote process that may be going on.

But I am sure that all members will take full opportunity to read your statements, to read the questions and the answers, and at this time I would recess the second panel and call up the third panel.

This panel is going to challenge me with the pronunciation of these names so I would take this opportunity to—Mr. O'Keefe, I can do yours, but I apologize to the other ones right up front. Dr. Zubeldia? Am I close?

Mr. ZUBELDIA. Yes.

Mr. BURR. And Ms. Koyanagi?

Ms. KOYANAGI. Yes.

Mr. BURR. Mr. O'Keefe and Ms. Meyer.

The Chair would recognize the good doctor to my right.

STATEMENTS OF KEPA ZUBELDIA, VICE PRESIDENT OF TECHNOLOGY, ENVOY CORPORATION; CHRIS KOYANAGI, DIRECTOR OF LEGISLATIVE POLICY, JUDGE BAZELON CENTER FOR MENTAL HEALTH LAW, ON BEHALF OF CONSUMER COALITION FOR HEALTH PRIVACY; MARK O'KEEFE, COMMISSIONER OF INSURANCE, DEPARTMENT OF INSURANCE, STATE OF MONTANA; AND ROBERTA MEYER, SENIOR COUNSEL, AMERICAN COUNCIL OF LIFE INSURANCE

Mr. ZUBELDIA. Thank you, Mr. Chairman. My name is Kepa Zubeldia. I am a physician, and I am here today representing the Association for Electronic Health Care Transactions, AFEHCT.

I am also vice president of technology for Envoy Corporation. Envoy is the largest medical transactions clearinghouse in the country. We process an average of 3.5 million transactions per day and provide connectivity between 270,000 providers and 800 payers.

We have been processing administrative transactions for 17 years; 62 percent of all health care claims are processed electronically today. The AFEHCT member companies take the issue of privacy very seriously. Since 1982 we have processed over 15 billion transactions. No AFEHCT member has experienced an instance in which protected health information was disclosed without authorization or in which an individual was harmed.

My written testimony addresses several issues of importance to your committee. First, the need for preemption to establish a single national law protecting patient privacy and facilitating the privacy of administrative records.

Second, the desirability of a consolidated patient consent for the transfer of personal and identifiable information.

Third, the need to support industry-driven security measures such as the standards adopted by the Secretary of HHS under HIPAA.

And fourth, the encouragement of the use of nonidentified patient information for medical research. I would center my remarks on two of these four issues.

First, the strong preemption of State law. The member companies of AFEHCT agree that protected health information should be granted the best protection necessary to keep the information confidential. Most health plans are administered at the national level. In order to accommodate the flow of information, it is imperative that national rules govern.

Subjecting administrative health care information to a multitude of State-specific requirements would cause harm to the processing infrastructure with immediate and significantly negative consequences for providers and payers alike. Health care is provided locally but administered nationally. We believe that preemption in this field will facilitate patient care, health care operations, and health research enormously. Individual patient's rights should not be based on an accident of geography.

My second topic is research. Legislation should encourage the creation of nonidentified data in order to accommodate the analysis of hundreds of millions of bytes of electronic data that can be gathered through various systems of collection each year. It is well to distinguish this potential for creating non-identified data on the electronic arena from the use of private patient records in clinical research.

In the majority of the circumstances, certainly consent should be obtained for the use of identifying private health information. We have heard much testimony regarding the proper times for an exception to the consent rules in dealing with identifiable protected health information in research situations. This is a different case, however, from the growing ability to create nonidentified information from electronic records of health transactions and employ this unanimously aggregated data in health research.

We believe that this approach provides both patient privacy and a powerful research tool to help reduce the cost of health care and should be favored by legislation. I wish to thank the chairman and members of the committee for the opportunity to speak to you today on behalf of AFEHCT, and I look forward to working together with you and your staff on these very important issues.

[The prepared statement of Kepa Zubeldia follows:]

PREPARED STATEMENT OF KEPA ZUBELDIA, VICE CHAIR, ASSOCIATION FOR ELECTRONIC HEALTH CARE TRANSACTIONS

Mr. Chairman, members of the Committee, Ladies and Gentlemen, good morning.

My name is Kepa Zubeldia, I am here today speaking on behalf of the Association For Electronic Health Care Transactions (AFEHCT). I currently serve as Vice Chair of AFEHCT, which is a trade association whose member companies are actively involved in the electronic transmission of health care financial and administrative transactions. These transactions include claims and patient encounter information, electronic remittance advice, eligibility, referrals, and related transactions listed in section 1173(a)(2) of the Social Security Act as amended by the "Administrative Simplification" provisions of the Health Insurance Portability and Accountability Act (HIPAA). An AFEHCT membership list is in Attachment A of my written testimony.

I am also Vice President of Technology for ENVOY Corporation, which is an AFEHCT member. ENVOY is a healthcare administrative transactions clearinghouse. We receive the administrative transactions specified under HIPAA, process them to ensure they have complete and correct information, and forward them to the health plan for payment. ENVOY is the largest medical transactions clearinghouse in the country, processing an average of 3.5 million transactions per day and providing connectivity between 270,000 providers and 800 payers. We have been processing administrative transactions for 17 years, with an accumulated experience totaling billions of transactions. Our corporate office is in Nashville, Tennessee, with sales offices in 14 states, data processing centers in 6 states, and a roster of about 1,000 employees. We have recently become part of Quintiles Transnational Corp., a diversified contract health organization based in Research Triangle Park, North Carolina, with over 17,000 employees in 31 countries.

Clearinghouses

ENVOY and other clearinghouse members of AFEHCT receive electronic transactions from providers, payers and vendors. The transactions are processed to ensure they are complete and accurate, and are then forwarded to the appropriate insurer or health plan. By processing these transactions electronically, rather than in paper format, a managed care referral or authorization, or a determination of eligibility and benefits can be obtained on a real-time basis, allowing patients to receive needed health care quickly.

Electronic claims represent a significant portion of the electronic transactions processed by ENVOY and other such clearinghouses. The charts in Attachment B of my written testimony show the growth of electronic claims. Sixty two percent (62%) of all healthcare claims are processed electronically with over 80% of hospital and pharmacy claims being processed electronically. Out of last year's total of 4.4 billion claims, 2.7 billion were processed electronically by ENVOY and other clearinghouses. Members of AFEHCT are intimately involved in administrative simplification that is currently saving the country billions of dollars in health care costs.

Support for privacy

The AFEHCT member companies take the issue of privacy very seriously. Since 1982, we have processed over 15 billion transactions. We actively protect the confidentiality of the protected health information that we process. No AFEHCT member has experienced an instance in which protected health information was disclosed without authorization or in which an individual was harmed. Indeed, we support a strong federal statute addressing privacy and confidentiality, and are actively involved in the privacy and confidentiality issues being addressed by your Committee.

In that spirit I would like to speak on several issues of importance to your Committee: the need for preemption to establish a single national law protecting patient privacy and facilitating the privacy of administrative records; the desirability of a consolidated patient consent for the transfer of personally identifiable information; the need to support industry driven security measures such as the standards adopted by the Secretary of HHS under HIPAA; and the encouragement of the use of non-identified patient information for medical research.

Strong preemption of state law

The member companies of AFEHCT agree that protected health information should be granted the best protection necessary to keep the information confidential. Most health plans are administered at the national level by a network of payors, third party administrators, administrative services organizations, peer review sys-

tems, foundations for quality review, and actuarial services. In order to accommodate the flow of information over these national electronic systems, it is imperative that national rules govern. It would be a daunting burden for the current payment system if local laws were able to create differing regulations for the processing and analysis of electronic records. Subjecting administrative healthcare information to a multitude of state specific requirements would cause harm to the processing infrastructure with immediate and significantly negative consequences for providers and payors alike.

The member companies of AFEHCT believe that private health information should be granted the best protection possible. We strongly support the desires of the states to protect medical record information, which we believe can best be accomplished through a comprehensive federal statute that sets out clear unified guidelines for the handling of the millions of electronic claims that cross all state lines.

It is a favorite truism that health care is provided locally but administered nationally. The system receives its funding on a national basis and record keeping of the providers and payors is accomplished on a national basis. We believe that preemption in this field will facilitate patient care, health care operations and health research enormously. Individual patient's rights should not be based on an accident of geography.

Consolidated patient authorization

To operate the intricate electronic system described above, it would be impossible for clearinghouses to obtain consent from the patient for each transfer of personally identifiable information along the communication channel between the provider and the health plan. Therefore, AFEHCT urges that legislation endorse a consolidated consent provision to facilitate this process. The general authorization granted by the patient at the point of health plan enrollment should stand as this consolidated consent. It provides clear notice to the patients of the handling of their claims information, as well a unitary guideline for all handlers of electronic data expressing personally identifiable health information.

Preserve administrative simplification provisions of HIPAA

We need to develop and employ from existing technologies the very best practices in encoding data so as to make sure patient privacy is strictly protected. Legislation before the Senate HELP Committee is takes steps in this direction. We believe that the health care industry should be given great incentives to adopt the highest standards for encoding electronic data and to use non-identifiable patient information for research. We support the Secretary of Health and Human Services in her effort to adopt industry driven standards as the standards adopted under HIPAA, rather than creating new standards.

Research

We agree with the stated purpose of the bipartisan legislation being considered this week in the Senate Committee on Health Education, Labor and Pensions (HELP) to encourage the use of non-identified health information, both in its creation by a recipient who is authorized to receive it and in its broad application by health researchers. This is a sensible way to increase the ability of researchers to create ever more powerful analytical studies while preserving patient privacy rights. The increased use of non-identifiable health information is a particularly attractive approach in the field of healthcare transactions because the immediate ability to encode information permits rapid access on an anonymous basis for health researchers. Therefore, legislation should encourage the creation of non-identified data—which does not require the further consent of the patient—in order to accommodate the analysis of hundreds of millions of bits of electronic data which can be gathered through various systems of collection each year.

It is well to distinguish this potential for creating non-identified data in the electronic arena from the use of private patient records in clinical research. In the majority of circumstances, certainly, consent should be obtained for the use of identified private health information. You will no doubt hear much testimony regarding the proper times for an exception to the consent rules in dealing with identifiable protected health information in research situations. That is a different case, however, from the growing ability to create non-identified information from electronic records of health transactions and employ this anonymous aggregated data in health research. We believe that this approach provides both patient privacy and a powerful research tool to help reduce the cost of healthcare, and should be favored by legislation.

Conclusion

In conclusion, in order to protect patient privacy, enhance the accurate and rapid administration of healthcare transactions, and to fulfill the aims of health research, it is important that:

- Federal standards, with state preemption, should be required to keep secure and confidential all identifiable health information including any administrative transactions that utilize identifiable health information;
- General authorization by means of a consolidated patient consent at the point of health plan enrollment should be adequate for the use of protected health information for purposes of treatment, payment and health care operations;
- The new legislation should not override, but support the security measures adopted by the Secretary of Health and Human Services implementing the Administrative Simplification of HIPAA;
- Conversion from personally identifiable information into non-identifiable information for the purposes of health research should be encouraged, while preserving the patient's privacy and without specific consent.

I wish to thank the Chairman and the Members of the Committee for the opportunity to speak to you today on behalf of AFEHCT. I look forward to working together with you and your staff on these very important issues.

ATTACHMENT A

AFEHCT

ASSOCIATION FOR ELECTRONIC HEALTH CARE TRANSACTIONS

Thomas J. Gilligan, Executive Director & Washington Representative; 3513 McKinley St. NW, Washington, DC 20015-2513, Tel (202) 244-6450, Fax (202) 244-6570, E mail afehct@aol.com

MEMBERSHIP

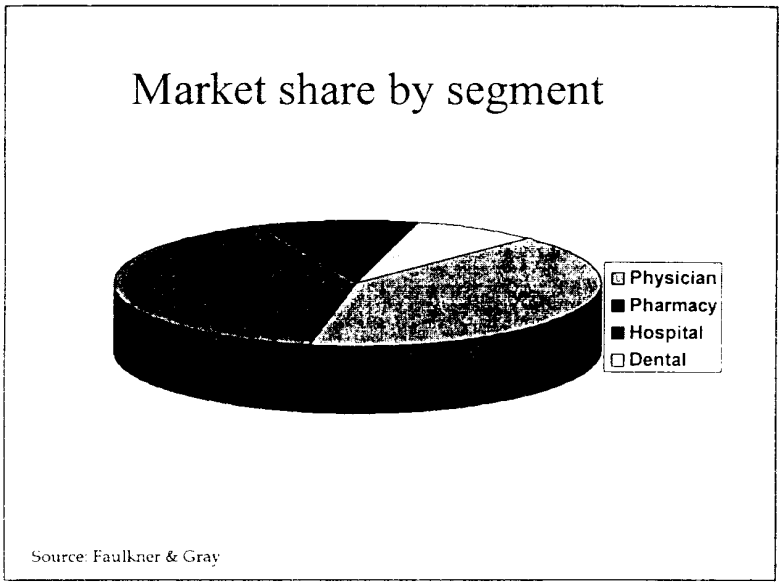
The Association For Electronic Health Care Transactions (AFEHCT) is a trade association, the membership of which include: health claims clearinghouses; health insurers; value added networks; software vendors; health care data processing companies; practice management companies; data communications systems operators; and credit card issuers.

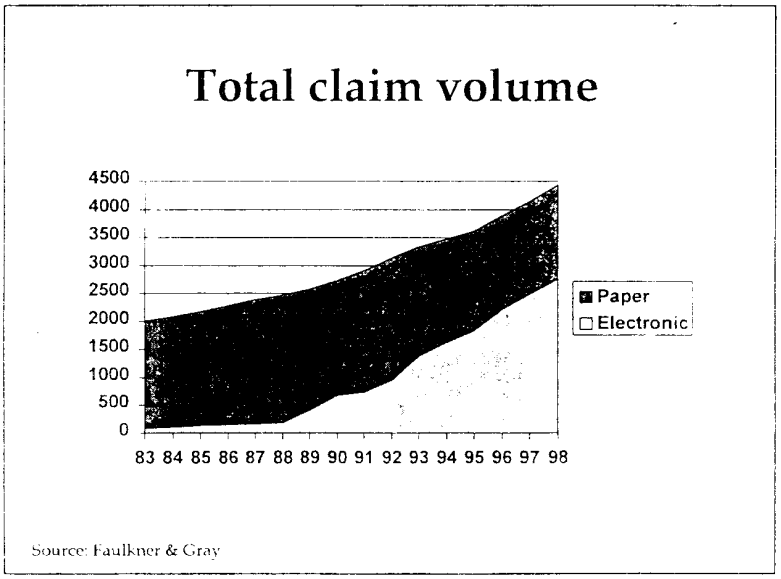
Each of these member companies is involved in the electronic transmission of health care financial and administrative transactions such as those listed in section 1173(a)(2): Health claims or equivalent encounter information; Health claims attachments; Enrollment and disenrollment in a health plan; Eligibility for a health plan; Health plan premium payment; First report of injury; Health claims status; and Referral certification and authorization.

AFEHCT MEMBERSHIP LIST

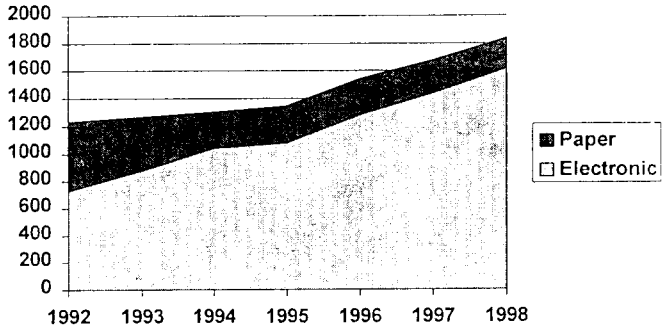
ANTHEM, Indianapolis, IN; BC/BS OF GEORGIA, Columbus, GA; BEACON PARTNERS, Hoffman Estates, IL; CARE-FULL SOLUTIONS, Cecil, PA; CONSULTEC, Tallahassee, FL; DIFFERENTIAL INC., Cupertino, CA; EDI-COMM, Woodland Hills, CA; EDS, Plano, TX; ELECTRONIC CLAIMS SERVICE INC., Houston, TX; EMPIRE BLUE CROSS, Syracuse, NY; ENVOY CORPORATION, Nashville, TN; HBO & CO, Atlanta, GA; IDX, Malvern, PA; HEALTHEON, Santa Clara, CA; IBM, Tampa, FL; INTEGRATED VISION SYSTEMS, Sebastion, FL; IVANS, Tampa, FL; JOHN DEERE HEALTH CARE INC., Moline, IL; MASTERCARD INTERNATIONAL, Purchase, NY; MEDAPHIS, Elgin, IL; MEDIC COMPUTER SYSTEMS, Raleigh, NC; MEDE AMERICA INC. Mitchell Field, NY; M & M COMPUTER SYSTEMS, San Antonio, TX; NATIONAL DATA CORPORATION, Atlanta, GA; PASSPORT HEALTH COMMUNICATIONS, Nashville, TN; PARAMORE CONSULTING, Louisville, KY; POINTSHARE, Seattle, WA; PRAGMATIX, Elmsford, NY; QUADAX, INC., Cleveland, OH; STERLING COMMERCE, Dublin, OH; TERBUSH & PARKER SYSTEMS, Richmond, VA; THE CENTRIS GROUP, Atlanta, GA; THE HEALTH INFORMATION NETWORK CONNECTION (THINC), New York, NY; UNISYS, Fairfax, VA; VISA INTERNATIONAL, San Francisco, CA; and WELLPOINT, Los Angeles, CA.

ATTACHMENT B



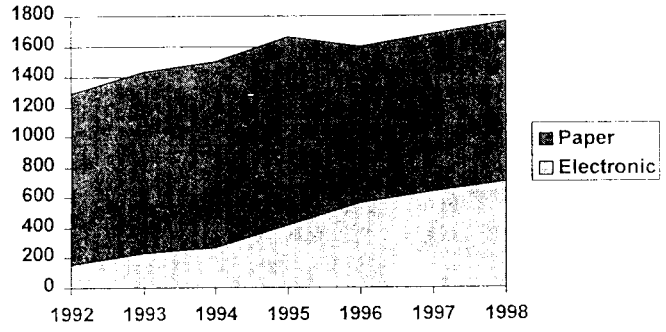


Pharmacy claims



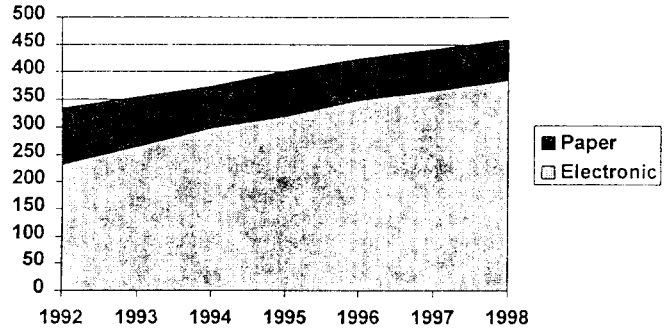
Source: Faulkner & Gray

Medical claims



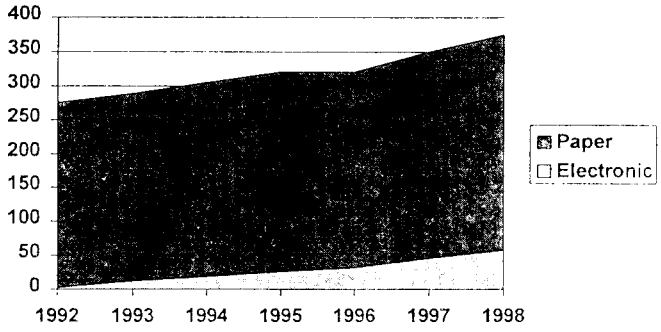
Source: Faulkner & Gray

Hospital claims



Source: Faulkner & Gray

Dental claims



Source: Faulkner & Gray

Mr. BURR. Thank you, doctor.

The Chair would recognize Ms. Koyanagi.

STATEMENT OF CHRIS KOYANAGI

Ms. KOYANAGI. Right, thank you, Mr. Chairman.

I am speaking today for a coalition of consumer and patient groups, the consumer coalition concerned with health care privacy. I wanted to begin by saying that we have talked a lot about research this morning, but in terms of health care delivery, privacy is a very, very important fundamental factor.

Some of the concerns that our group has is that, in fact, the quality of health care is affected if individuals are not assured of the privacy of the medical information. A recent survey in California looking at this issue found that as many as one in six people will engage and do engage in behaviors to protect themselves because they fear that their medical records will leak out.

They doctor shop, they withhold information, they give part of the information, or they don't provide information to their treating professionals perhaps not understanding what some of the consequences of that might be. But that means that this is a very, very critical area and that patient confidence is very, very important in response to the legislation that you pass.

I was asked today to talk specifically about the issue of preempting State laws. I want to say first that a strong Federal floor is something that we clearly endorse and urge you to enact. That will give patients much greater confidence with respect to the privacy of their information.

On the other hand, there is a lot of reasons to continue to permit States to act in this area. The strong Federal floor in any of the bills, any of the major bills being considered in the House or the Senate, represent a strong Federal floor compared to all of the existing State laws.

Most of the provisions in current State laws would be overridden by any of the bills pending in the committee. So we are talking about a few provisions; and, in fact, we are talking about not all of the States in terms of having stronger provisions for privacy than might be in the Federal legislation.

Earlier somebody was discussing the fact that States had moved into this area because there is no Federal legislation. I think that is very true. I think that States have been forging new ground in a very complex arena. If there were a Federal statute, I think it very, very likely that you would see great uniformity across the country, that many States would conform their legislation to the Federal legislation, and they would go beyond it only in specific areas for specific reasons.

For example, Vermont right now has a cancer registry. They want specific rules around privacy for that registry. They should retain the flexibility when they have a situation like that that is not addressed in the Federal law to have their own provisions to protect their own citizens. I think it is important to continue to negotiate these things on the State level.

State legislatures do know their own local situation. They do balance the interests of, say, a research entity in the State and their citizens concerns. They can go back and amend legislation. As you

heard this morning, the Maine legislation was withdrawn almost immediately when it was realized that they had made mistakes and gone too far. The Minnesota legislation has been amended once. If there are significant concerns and if the citizens of Minnesota think that it has gone too far, I assume it will be amended again.

But many things happen very quickly, much more quickly than the Congress can respond. We don't know where we are going in this area. With the explosion of technology and access through the Internet, things are happening today that we never would have dreamed much a year ago. I think that it is very important because privacy is such a fundamental aspect of patient care and good quality of care, and it is a fundamental concern of Americans to have privacy in areas where they don't believe others should be intruding.

I think it is very important that the States continue to have that kind of flexibility and to act quickly. So we would urge you to go ahead and pass a strong Federal floor, but to resist the temptation to make it a ceiling.

Just in closing, I would point out that there are other industries where you have done this. The banking industry operates where States can go beyond the Federal statute, and the same is true for credit card regulations.

So in conclusion, that is our recommendation, that you enact a floor but not a ceiling. Thank you.

[The prepared statement of Chris Koyanagi follows:]

PREPARED STATEMENT OF CHRIS KOYANAGI, POLICY DIRECTOR, JUDGE DAVID L. BAZELON CENTER FOR MENTAL HEALTH LAW ON BEHALF OF THE CONSUMER COALITION FOR HEALTH PRIVACY

I. INTRODUCTION AND OVERVIEW

Mr. Chairman and Members of the Committee: I very much appreciate the opportunity to testify before you today on the preemption of state laws relating to medical privacy, confidentiality, and security. I am Chris Koyanagi, Policy Director for the Judge David L. Bazelon Center for Mental Health Law in Washington D.C. The Bazelon Center is a legal advocacy organization concerned with the rights of persons with mental impairments.

I testify today on behalf of the Consumer Coalition for Health Privacy (CCHP), a broad coalition of consumer, disability and patient advocates. The mission of the Consumer Coalition for Health Privacy is to educate and empower healthcare consumers to have a prominent and informed voice on health privacy issues at the federal, state, and local levels. Members of the coalition are committed to the development and enactment of public policies and private standards that guarantee the confidentiality of personal health information and promote both access to high quality care and the continued viability of medical research. The Coalition is an initiative of the Health Privacy Project, Georgetown University Medical Center.

As a member of the Coalition's Steering Committee, I have been working with my colleagues in the disability rights, consumer, and patient advocacy communities to make the case that protecting privacy must be a "first principle" of enhancing the quality of health care, of fostering research and public health initiatives, and of broadening access to critical health care services. We believe that 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.

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."[1] 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.

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.

Members of the Consumer Coalition are keenly aware of the importance of good, solid data for research. As health care patients and providers, our members stand to benefit the most from advances in research, public health initiatives, and improvements in quality of care. People with disabilities, in particular, are frequent users of health care services, and are also deeply invested in ensuring that the health care system operates efficiently and effectively. As such, the Consumer Coalition for Health Privacy is committed to ensuring that protecting privacy and promoting health are values that must go hand-in-hand.

Towards this end, the Consumer Coalition has established a set of health privacy principles to guide our efforts (see attached principles and sign-on). We believe that public policy in this area should guarantee individuals: a right to see their own medical records; the ability to exercise voluntary, informed choices about the use of their health information; a court order or warrant requirement for law enforcement access to medical records; and a comprehensive set of enforcement mechanisms.

We hope that Congress will meet the deadline established in the Health Insurance Portability and Accountability Act (HIPAA) to pass comprehensive health privacy legislation by August 1999, and we also hope that the new law will go a long way in helping us to meet these public policy goals set forth in our principles. However, in many ways, one of the most critical issues for the Coalition is preemption. *The Coalition arrived at a firm consensus that "federal legislation should provide a floor for the protection of individual privacy rights, not a ceiling."*

At issue here is how a federal health privacy law will relate to existing and future stronger state laws. 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?

The two comprehensive health privacy bills pending in House—The Health Information Privacy Act, co-sponsored by Reps. Waxman(D-CA), Condit (D-CA), and Markey (D- MA), and H.R.1057, The Medical Information Privacy and Security Act, introduced by Rep. Markey (D-MA)—would both set a federal preemptive floor, eliminating weaker state laws, and allowing states to continue to enact heightened protections where necessary to guard against public health threats.

Both bills mirror the Coalition's principle on preemption. However, a number of other proposals do include some form of preemption of stronger state laws. Most notably, a provision in the Patient Protection Act of 1999 (H.R. 448) includes very broad preemption language. Particularly troubling is that it would preempt stronger state laws relating to authorization for "health care operations" without replacing them with a meaningful set of federal protections.

In addition, a bill scheduled to be marked-up in the Senate HELP Committee would preempt certain stronger state laws in the future, grand-fathering in existing stronger protections. Again, we strongly oppose federal preemption of state laws that provide greater consumer protections—including heightened safeguards for certain medical conditions and circumstances. Our testimony today is intended to dem-

---

[1] The poll was conducted for the Foundation by Princeton Survey Research Associates. The survey topline is available at http://www.chcf.org.

onstrate that the federal law should establish a floor of protections, not a ceiling. We believe that a fully-preemptive federal law in this area is unprecedented, unwise, and may be a danger to public health.

Our testimony highlights specific state laws at risk of being preempted under a total preemption approach. It should be emphasized, however, that preemption is a moving target. Until there is a consensus bill, it will be impossible to determine the full impact of preemption.

The Consumer Coalition for Health Privacy opposes the preemption of stronger state laws for the reasons outlined in this testimony.

II. THE NEED FOR UNIFORMITY

Congress will create a high level of uniformity by preempting weaker state laws. Passage of proposed federal health privacy bills will result in substantially greater uniformity, given that all the proposals preempt weaker state laws. Simply by preempting these weaker state laws, Congress will eliminate the vast majority of state laws and create a high degree of uniformity.

Preliminary research on state health privacy laws conducted by the Health Privacy Project shows that most state laws governing the broad areas sought to be regulated by the federal bills—patient access to records, notice of information practices, patient authorization for disclosure, remedies for violation of the law—would fall under the floor laid down by the House proposals.

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—and often conflicting—state laws. At the same time, the vast majority of these laws are weaker than the standards proposed in most the pending bills. Therefore, far from adding additional burdens, the federal law will provide a substantial degree of uniformity simply by preempting weaker state laws. A federal floor—if it is set at an appropriate level—will actually standardize the vast majority of health privacy and security practices.

Moreover, *there is no evidence that the interplay between state and federal laws in these areas significantly interferes with interstate commerce.* The Right to Financial Privacy Act, the Fair Credit Reporting Act, and the Electronic Communications Privacy Act regulate the banking, credit, and communications industries, all of which conduct extensive business across state lines. All of these laws, however, leave states free to enact more protective laws as they see fit.

III. PRECEDENT IN FEDERAL CIVIL RIGHTS AND PRIVACY LAW

No precedent exists in federal privacy or civil rights law for preempting stronger state laws. In the past, when Congress has considered preemption, it has recognized the importance of allowing states to address issues unique to the states and their citizens. Historically, the federal government establishes a "floor" of protections, leaving the states free to provide greater protections.

The proponents of total preemption express fear that states will pass laws that are "too privacy protective," thereby interfering with important health-related activities. But the facts are reassuring: states have been quick to respond to the concerns of health care plans, researchers and others. *Where a "privacy protection" was deemed to interfere with vital health care functions, states have quickly amended their laws.* Minnesota, for example, amended a law relating to researcher access to medical records after hearing objections from health care organizations in the state. More recently, Maine postponed implementation of a health privacy law after objections on the part of press and family members.

Many states are considering pending health privacy bills, in an attempt to fill the vacuum created by the existing gap in federal health privacy law. However, in the past, following the passage of comprehensive federal legislation, the momentum behind such state initiatives drops significantly. After passage, state activity is likely to reflect the standards proposed in the federal law, thereby increasing uniformity.

IV. STATE LAWS MORE DETAILED AND NUANCED

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 issues traditionally acted on at the state level that include privacy provisions. These include anti-discrimination laws, commitment proceedings for the mentally ill, adoption, foster care, mental health treatment, re-

productive health, parental involvement, partner notification, and abuse and neglect.

In comparison, the federal proposals have, on the whole, treated all health care organizations in a similar fashion. The federal proposals have also established—with a broad brush—general rules about the use or disclosure of health information. These rules will address the vast majority of circumstances in which health information is used and disclosed, but they do not approach the level of detail that has been developed at the state level over many years.

- California law provides patients a right to see and copy their own medical record, as do all the Senate proposals. The state law, however, also explicitly provides that access can not be denied because the individual owes money for past services.[2]
- 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 that participate in an approved plan of a core service agency[3] for the delivery of mental health services *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*.[4]
- Vermont requires the Health Commissioner to maintain a cancer registry and to keep all information confidential, except in limited circumstances.[5] Most of the Senate bills *would allow for greater disclosure* of the information maintained in the registry than is currently permitted under Vermont law. Many states have established similar cancer registries by statute.

Such a level of detail is not even contemplated by any of the federal proposals, and regulating these spheres is clearly not the intent of any of the federal proposals. By fully preempting state law, Congress would likely preempt important state laws without providing an equal level of guidance, or necessary protections.

V. VALUE OF "HEIGHTENED PROTECTIONS" AT THE STATE LEVEL

Most of the pending proposals treat health information the same. Unlike the state laws, the proposals do not establish specific rules for certain kinds of information. However, the Waxman-Condit-Markey bill does allow for heightened protections for especially sensitive information.

The result is that even the strongest federal proposals have not set the bar as high as some state laws. If any of the current federal health privacy proposals were to pass with a preemptive federal ceiling included, the citizens of some states would actually forfeit the protections they are now guaranteed under their state laws.

- California has enacted a number of HIV/AIDS specific confidentiality laws, covering testing, reporting, partner notification, and discovery. 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.[6]
- In Georgia, heightened protection is given to information derived from genetic testing. 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.[7]

---

[2] California Health and Safety Code, Section 123100 et seq.

[3] A "core service agency" is an organization approved by the Mental Hygiene Administration to manage mental health resources and services in a designated area or to a designated target population. Md. Health-General Code Ann. Sec. 4-307(a)(3) (1999).

[4] Maryland Id. At Sec. 4-307 (e).

[5] 18 V.S.A. Sections 154 et seq.

[6] See California Health and Safety Code, Section 120975 et seq; 121015 et seq, Insurance Code, Section 799 et seq.

[7] Ga. St. 33-54-3.

- New York has a comprehensive set of statutes providing additional protection of the confidentiality of HIV related information. New York generally prohibits the disclosure of HIV related information without the patient's consent. Accordingly, a patient's consent to the release of HIV related information specifically limits to whom disclosure may be made, the purpose for such disclosure and the time period during which the release is effective. *Unlike the federal proposals, a general authorization for the release of medical information does not encompass the disclosure of HIV related information unless it specifically states so.*[8] In enacting these statutes, the New York legislature expressly stated that it intended to "encourage the expansion of voluntary confidential testing for . . . HIV so that individuals may come forward, learn their health status, make decisions regarding the appropriate treatment, and change the behavior that puts them and others at risk of infection."[9]
- Tennessee law stipulates that the State Department of Health records on STDs may not be released even under subpoena, court order, etc. unless the court makes a specific finding concerning each of five criteria including: weighing 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.[10]

Many states have laws similar to the ones cited above for certain information such as mental health, genetic tests, and HIV/AIDS. Again, none of the federal proposals reach these levels of protection. In some circumstances, states enacted these heightened protections to respond to critical public health issues. 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.

VI. THE DANGER OF UNINTENDED CONSEQUENCES

Laws relating to the confidentiality of medical information are found throughout state codes. In California, for example, citizens have a right to privacy in the State Constitution. 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 discreet 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 not possible to predict in advance the full impact of such broad preemption on state law and consumer protections. The "relating to" language used to preempt state law in some federal proposals casts a wide net in terms of the state laws that would be eliminated completely. *The preemption of all state law "related to" the federal law could have significant unintended consequences.*

- At risk of being preempted is 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.[11]

A larger issue is at hand. Many state health privacy laws were enacted specifically to address public health concerns. Mental health and HIV/AIDS confidentiality laws, for example, were enacted specifically to encourage people to seek appropriate care, without fearing harmful reprisals.

The states are best equipped to respond to many 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.

---

[8] NYCLS Public Health Law Sec.2780 et seq.
[9] NY Laws 1988, ch 584, Sec. 1.
[10] Tenn. C.A. Sec. 68-10-113 6(A).
[11] Insurance Code, Section 10140 et seq.

VII. CONCLUSION

Most importantly, Congress will create a high level of uniformity simply by preempting weaker state law with a strong federal law. This is true under most of the Congressional health privacy proposals' the research of state health privacy laws bears this out. Thus, there is no overriding justification to totally preempt state law in order to achieve substantial uniformity.

The interests of health care consumers and providers will be best served by Congress establishing a federal floor that leaves the states free to enact greater protections, as Congress has done for every other privacy and civil rights laws, regardless of how complex or interstate the area to be regulated. Such a solution would allow the states to address the specific—and unique—needs of their citizens while providing a great deal of national uniformity regarding the use and disclosure of health information. A federal ceiling, on the other hand, could have profound negative consequences for consumers and health care providers by inadvertently eliminating important protections, or restricting the ability of states to respond to the privacy needs of their residents.

Passage of a federal health privacy law will necessarily involve compromises. The stakeholders are diverse, as are the states and their constituencies. It is appropriate that the federal law would reflect these compromises, but it raises a troubling possibility: that the federal law will set a relatively low standard *and* preempt state law. This is the worst-case scenario. The result would be to eliminate existing state protections without replacing them with comparable federal standards, locking the states out of taking steps to address local health needs.

We urge this Committee, and the rest of the Congress, to resist the proponents of total preemption. Such a radical approach would undo legal protections put in place by states responding to pressing public health concerns.

In order to encourage people to seek testing, counseling, treatment, and other health care services, many states have established heightened protections for people with mental illness, HIV/AIDS, drug and alcohol dependence, and other circumstances where people face stigma, discrimination, and embarrassment. If these safeguards were wiped off the books, as they would be under H.R. 448, the most vulnerable people in our communities would immediately be put at risk of exposure, and faced with the cruel choice of either protecting their privacy or seeking health care. Such a result, we believe, would substantially undermine state—and national—health initiatives.

Rather than undermining our nation's existing system of checks and balances, we should continue the tried and true practice of allowing states to decide when it is appropriate to provide consumer protections stronger than the federal law.

Mr. BURR. We thank you for that testimony. And there will be some question as to whether the banking industry, after today's mark up, you could still say that about.

I would also make one point that Maine did have the ability to react quickly. We have not found this institution to have the ability to fix mistakes very quickly other than the legislative process, so I hope we will all attempt to get it right the first time.

Mr. BROWN. Mr. Chairman, we did today, when the House adjourned. Never mind.

Mr. BURR. The gentleman just missed his questions.

Mr. O'Keefe.

Mr. O'KEEFE. Mr. Chairman, members of the committee, let me begin by asking to submit a letter from the National Conference of State Legislatures for the record, if I could.

Mr. BURR. Without objection so ordered.

[The information referred to follows:]

NATIONAL CONFERENCE OF STATE LEGISLATURES
WASHINGTON, DC
May 27, 1999

The Honorable THOMAS J. BLILEY, JR.
Chairman, Commerce Committee
U.S. House of Representatives
Washington, D.C. 20510

DEAR CHAIRMAN BLILEY: On behalf of the National Conference of State Legislatures (NCSL), I would like to take this opportunity to briefly comment on federal proposals regarding medical records confidentiality. NCSL will be submitting more detailed testimony for the record at a later date.

NCSL firmly believes that states should regulate insurance. That being said, we recognize that there is a legitimate role for the federal government, particularly regarding the development of uniform national standards that establish a basic level of protection for consumers nationwide. Federal medical records confidentiality legislation should provide every American with a basic set of rights regarding their health information. These federal standards, in concert with state law, should be cumulative, providing the maximum protection for our citizens. At the end of this process, when federal legislation has been enacted, I hope we will be able to say that not one individual's health information is more vulnerable on that day, under federal law, than it was the day before without it.

Preemption of State Law

Federal law 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, education, juvenile justice, criminal code, civil procedure, family law, labor and employment law. There is currently no compendium of state confidentiality laws. NCSL continues to work with Georgetown University where a major effort to produce such a compendium is underway. A blanket preemption of state law is virtually the same as throwing the baby out with the bath water.

If there is going to be preemption of state law in federal medical records confidentiality proposals they should: (1) grandfather existing state 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 states to enact legislation that provides additional protections. If states are precluded in some general way from taking action in specific areas, there should be a mechanism for a state legislature to act, if the federal legislation adversely impacts the citizens in the state due to a technical error in the legislation or to unintended consequences based on state-specific conditions.

Some of the federal proposals have attempted 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 enact legislation. While well-intentioned, each bill has a different set of carve-outs and we have no way of knowing the full extent and impact of the preemption and carve-outs until the federal law has been implemented. In other words, we won't know what has been missed until after the federal law is enacted. NCSL and the National Association of Insurance Commissioners (NAIC) recommend another approach. If an issue is not specifically addressed in the federal law, states may continue to legislate and regulate in the area. 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

Through the end of April 1999, sixteen states have enacted laws regarding medical records confidentiality. We will provide an update that will include actions taken by states that have ended their sessions since the end of April in our more detailed testimony that we will submit for the record. Montana enacted comprehensive legislation addressing the activities of insurers and North Dakota enacted legislation that established comprehensive public health confidentiality standards. Most of the other 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, Georgia, Idaho, Mississippi, Nebraska, Nevada, New Mexico, Oklahoma, South Dakota, Utah, West Virginia and Wyoming.

Several of these new laws address issues that are not addressed in many of the federal proposals. For example, 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. 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. These are but a few examples that illustrate both the breadth and complexity of the preemption issue.

I thank you for this opportunity to briefly share the perspective of state legislatures on this very important issue and 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 Americans.

Sincerely,

WILLIAM POUND
Executive Director

cc: Members, House Commerce Committee

STATEMENT OF MARK O'KEEFE

Mr. O'KEEFE. I am Mark O'Keefe. I am the elected State auditor from the State of Montana, Montana being a fiscally conservative State. I also serve as securities commissioner and, for the purposes of this hearing today, insurance commissioner for the State of Montana and have for the last 7 years.

It is a pleasure to be here this afternoon. I appreciate the opportunity to discuss medical records confidentiality with you.

I would like to make some brief comments recognizing the desire for a minimum Federal standard. I will then address the need for Congress to clarify the scope of any Federal health information privacy legislation. And finally, I want to discuss the enforcement issue which may seem to go beyond preemption; but as you will see, I believe actually gets to the heart of whether or not Congress ought to adopt a floor in this area or completely preempt the States.

Mr. Chairman, members of the committee, the NAIC have recognized that you must act in this area. As required by HIPAA, you have to have privacy legislation by August 21 or we have regulations from health and human services. In addition to this, the European Union passed Directive 9446-EC which is a privacy directive that requires companies exchanging information with member companies to meet strict privacy standards. Commerce is now involved in negotiating those standards.

We have reviewed all of the legislation currently before Congress—and while we would prefer to see Congress enact a law that leaves all current State law in place, none of the bills offered gives

us this choice. Given this, the members of NAIC would prefer to see a Federal floor rather than a total preemption in the area.

State law in this area has not developed evenly. As far as we know, no State has enacted one health information privacy law that covers all aspects of health privacy. Rather a State enacts a privacy provision when dealing with school records, another for hospital records, a third for public health, et cetera, et cetera, et cetera. Completely preempting all State privacy laws may preempt many of these laws that are not covered by the new Federal standard leaving millions of consumers with few protections under State or Federal law.

Second, health information privacy covers a wide range of subjects, from mental health and HIV to substance abuse and battered spouses. Again preempting all State law could have the unintended consequences of leaving millions of consumers with fewer protections, not more.

Third, if the States are completely preempted in this area, they will not be able to respond to changes in technology or changes in the way information is used in the future. We feel the States, as your comments a little earlier reflected, react much quicker to what is going on than Congress does in regards to medical information.

As I mentioned in my written statement, a Federal preemption of State privacy laws would invalidate certain laws in my home State of Montana, but Federal preemption in my State goes even further. Montana's constitution contains an explicit right of privacy for the residents of our State. A total Federal preemption would conflict with the State constitutional guarantee of privacy.

Montanans across the board believe that medical records belong to the individuals whose records they are, not to some corporation. We know how the supremacy clause works, but we as Montanans have a strong belief that that is our belief.

Finally, Mr. Chairman, States should not be preempted because of the enforcement issue. While the Federal bills all include criminal sanctions for those who knowingly and intentionally disclose this information, it is unlikely many prosecutions will take place. States have a much bigger hammer. Insurers and other persons such as hospitals and providers are licensed by the States. This forces these weakened and—hold these licenses and make sure that these rights are protected by threatening to take them away.

A last point about enforcement is that the State departments of insurance offer consumers a place to go with their complaints. Right now in Montana, I receive an average of 45,000 calls a year with complaints against insurers and securities firms in my State. I have a population of 800,000. I am the responsible entity to deal with those complaints. Should the Federal law pass, whom do my 800,000 people call? Department of Labor in Kansas City? Department of Health and Human Services in Denver? States already have an enforcement operating plan, and we think it should stay in place.

With that, I would be glad to answer any questions you might have. We urge you to recognize the impact of this legislation on Federal and State laws as you debate the issue. Mr. Chairman, we look forward to working with the subcommittee, the committee, and the Congress in resolving these laws.

[The prepared statement of Mark O'Keefe follows:]

PREPARED STATEMENT OF MARK O'KEEFE, COMMISSIONER OF INSURANCE, STATE OF MONTANA ON BEHALF OF THE NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

I. INTRODUCTION

Good morning, Mr. Chairman and members of the Subcommittee. My name is Mark O'Keefe. I am the elected Insurance Commissioner for the state of Montana. I am testifying this morning on behalf of the National Association of Insurance Commissioners' (NAIC) (EX) Special Committee on Health Insurance. I would like to thank you for providing the NAIC with the opportunity to testify today about the preemption issue surrounding the health information privacy legislation currently before Congress.

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 45 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.

My testimony today will focus on three aspects of the preemption issue raised by the current federal legislation. First, I will discuss the states' recognition of the desire for a minimum standard to protect the privacy of health information. Second, I 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, I 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.

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. In addition to this statutory deadline, we recognize that Congress faces pressure to enact national legislation protecting the privacy of health information because the European Union issued a privacy directive that became effective in October 1998.

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] How-

[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

ever, 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 information 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 me give you some examples of the existing state laws that protect health information.

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

---

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.

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.).[4] 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.

Virginia—Virginia has already enacted a privacy protection law for insurance information. (Va. Code Ann. § 38.2-600 et seq.). This law applies to insurance institutions, agents and insurance-support organizations, and it protects insurance information, including 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, accident and sickness (health), and property and casualty insurance, and therefore to issuers of these products. The state law prohibits the disclosure of personal or privileged information about an individual, with some exceptions. 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 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 the Virginia law in some way, the level of protection for information held by life and health insurers would be diminished.

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 diagnosing 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.

Massachusetts—Under Massachusetts' education statutes, provisions are established for the testing, treatment and care of persons susceptible to genetically-linked

[4] Montana's Insurance Information and Privacy Protection Act is very similar to Virginia's law (see next section for more discussion).

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.

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.

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.

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.

Because state laws relating to health information and privacy are located in so many different places within each states' legal code, the length of time and complexity involved in compiling a list of these laws make it a nearly impossible task. Moreover, there is no federal or state agency or other organization that has a complete compendium of state laws that could be preempted by federal privacy legislation. Without clear information about the laws that may be impacted by legislation, preemption must be approached with caution.

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.[5] 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.

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 spe-

---

[5] 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 plan . . .* (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.

cific 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.[6] 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 explicitcategories 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. 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, HowHowever, 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 law 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

---

[6] As of Friday, May 21, 1999, the Chairman's Mark of S. 578 in the Senate Committee on Health, Education, Labor and Pensions (HELP) contained the following exceptions to the federal preemption language for certain state laws that: (1) relate to use and disclosure of information pertaining to mental health and pertaining to public health consistent with Section 207 to the extent that such state law prevents or restricts the use and disclosure for protected health information otherwise permissible under this Act; (2) relate to the disclosure of protected health information or any other information about a minor to a parent or guardian of such minor; or (3) concern a privilege of a witness or person in state court.

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.

Mr. BURR. We thank you, Mr. O'Keefe.

The Chair would recognize Ms. Meyer for her opening statement.

STATEMENT OF ROBERTA MEYER

Ms. MEYER. Mr. Chairman, Congressman Brown, my name is Robbie Meyer.

I represent the American Council of Life Insurance. The ACLI is a national trade association that represents about 493 companies which sell life insurance, disability income insurance, and long-term care insurance. We appreciate being given the opportunity to appear before you today.

The very nature of life insurance, disability income insurance, and long-term care insurance involves personal and confidential relationships. The ACLI is here today because these insurers use health information for essential business purposes. Life, disability income, and long-term care insurers must use health information to evaluate consumers' applications for insurance coverage and to process their claims for benefits.

The legislation to be considered by the subcommittee will govern how life, disability income, and long-term care insurers obtain, use and disclose health information. As a result, the actions of this subcommittee will impact fundamental and essential functions of our business. We are strongly committed to the principal that individuals have a legitimate interest in seeing that their personal information is properly collected and handled and that insurers have an obligation to insure individuals of the confidentiality of that information.

Medical information and a life, disability income, or long term care insurance file may be used for certain business purposes. It is used to underwrite applications for coverage. It is used to process claims. It is used in connection with reinsurance. And it is used, as stated by the previous witness, by State insurance departments on many occasions.

I would like to take this opportunity now to address just a couple of key concerns in some of the pending pieces of medical record confidentiality legislation. First, authorization and revocation. Every year America's life, disability income, and long-term care insurers enter into literally millions of contracts with American consumers. Insurers, as I said before, use health information in connection with those contracts to evaluate consumers' applications for coverage and also to process their claims. These contracts can be in effect literally for decades and often are.

Currently, we only access medical information with an individual's authorization. In other words, we only get information if they say that it is okay for us to get it. The current pieces of legislation that are under consideration now would not only require that authorization deal with our ability to get information but would also

govern our ability to use it and then to redisclose it as necessary in the ordinary course of business.

In order to prevent this legislation from inadvertently interfering with the industry's ability to perform essential yet ordinary business functions and—very importantly—to fulfill our contractual obligations to consumers. Life, long-term care, and disability income insurers need to be able to obtain a single authorization for disclosures of medical information only in connection with the ordinary course of business. And we need to have these authorizations remain valid for the lifetime of the contract so that we can fulfill our contractual obligations to our customers.

Other concerns we have with some of the pending pieces of legislation deal with the right to self-pay, damages, and preemption of course. Some of the bills would grant an individual to self-pay for certain treatment and then give them the right to prohibit or limit disclosure of information relating to that information.

We are very concerned that that would create a situation where there are conflicting authorizations and the health care providers, doctors and hospitals wouldn't be sure which rule will govern the authorization that the individual originally gave the insurer or the direction from the individual to hold back that information.

We are very concerned about any piece of legislation that would provide for punitive damages. And then, finally, as stated in our written statement and as I previously stated, we feel very strongly that American consumers have an absolute legitimate expectation that their health information will be kept confidential.

A Federal Statute that outlines broadly preemptive standards, specific standards and which provide remedies for breach of those standards, we believe will respond to the American public's concern about the confidentiality of their health information. We believe that setting a national uniform standard for health information is obviously fundamental to this debate.

Consumers would know what the rules were that would govern their health information regardless of where they lived. And insurance companies doing business across the country, as many of our member companies do, would be able to adhere to a uniformed standard, hopefully, be able to pass the economies of that uniform standard on to their customers. And we believe that this would very much facilitate insurers' ability to continue to provide financial security to American consumers.

One of the previous witnesses indicated a concern about the fact that people were scared of what was going to happen with respect to the confidentiality of their medical information and that they were concerned that if their medical information was out, that it would cause their insurance policies either to be canceled or for their rates to go up. I did want to respond to that since I had a few minutes.

The fact of the matter is that life, disability income, and long-term care insurers cannot cancel their policies and they cannot raise their rates because of the health of an individual. Disability income and long-term care rates can be raised, on certain occasions, for a group of insuredes but never because of the health of an individual.

With that, thank you very much. I would be glad to answer any questions.

[The prepared statement of Roberta Meyer follows:]

PREPARED STATEMENT OF ROBERTA MEYER, SENIOR COUNSEL, AMERICAN COUNCIL OF LIFE INSURANCE

INTRODUCTION

Chairman Bilirakis, Congressman Brown, and members of the subcommittee, I am Roberta Meyer, Senior Counsel at the American Council of Life Insurance (ACLI). I am pleased to discuss, and offer our assistance, as you craft legislation governing the confidentiality of medical record information. The ACLI is a national trade association with 493 member life insurance companies representing approximately 77 percent of the life, 81 percent of the disability income, and 88 percent of the long term care insurance in force in the United States. The fundamental purpose of life, disability income and long term care insurance is to provide financial security for individuals and families.

- *Life insurance* financially protects beneficiaries in the event of a person's death. Proceeds from a life insurance policy may help a surviving spouse pay a mortgage or send children to daycare or college.
- *Disability income insurance* replaces lost income when a person is unable to work due to injury or illness.
- *Long term care insurance* helps protect individuals and families from the financial hardships associated with the costs of services required for continuing care, for example, when someone suffers a catastrophic or disabling illness.

Every year America's life, disability income and long term care insurers engage in millions of contracts. Those contracts are the promises we keep to our policyholders.

The very nature of the life, disability income and long term care insurance businesses involves personal and confidential relationships. The ACLI is here today because life, disability income, and long term care insurers use health information for business purposes. We are well aware of the unique position of responsibility we have regarding an individual's personal medical information. We are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their health information and that insurers have an obligation to assure individuals of the confidentiality of that information. As an industry, life, disability income, and long term care insurers have a long history of dealing with highly sensitive personal information in a professionally appropriate manner. We are proud of our record as custodians of this information.

BACKGROUND

When a consumer begins the search for a life, disability income, or long term care insurance product, he or she usually begins by meeting with an insurer's sales representative. An individual may respond to an advertisement or the sales representative may initiate contact through a referral. Sales representatives usually meet with potential clients in their homes or at their place of employment. This is where the relationship between the insurer and the individual typically begins.

During this initial meeting, the sales representative will discuss with the individual their family's financial security needs. If the consumer decides to apply for an individually underwritten life, disability income, or long term care insurance policy, the sales representative will complete an application.

Many of the application questions concern nonmedical information, such as age, occupation, income, net worth, other insurance and beneficiary designations. Other questions focus on the proposed insured's health, including current medical condition and past illnesses, injuries and medical treatments. The sales representative also will ask the applicant to provide the name of each physician or practitioner consulted in connection with any ailment within a specified period of time (typically five years). Other questions will concern past use of alcohol and drugs, smoking habits and information about family history.

The sales representative usually asks the questions and records the proposed insured's responses. After the individual has reviewed the responses to be sure they are accurate and complete, he or she will sign the application. In certain cases, the applicant and the proposed insured may not be the same individual. This occurs when, for example, a parent (applicant) applies for coverage on a minor child (proposed insured) or when spouses apply for coverage on each other. In such cases, the

application for coverage will likely be signed both by the applicant and proposed insured.

Up to this point in the process, the information the insurance company receives about the proposed insured's health status is directly from the individual. Depending on the age and medical history of the proposed insured, and the amount of insurance applied for, the insurance company may require medical record information. When the sales representative takes the consumer's application for insurance, he or she also will *ask the individual to sign a consent form authorizing the insurance company to verify and supplement the information regarding the proposed insured's medical history, and to obtain additional information if it is needed* to evaluate the application. This additional information generally is held by the proposed insured's attending physician(s) or hospitals. If it appears that the insurance company will need this information for the underwriting process, the insurance company will send to the physician or hospital the signed authorization. The insurer will reimburse the provider or hospital for the administrative expenses in locating and sending a copy of the information to the insurer.

The medical information that insurance companies typically request of applicants include routine measurements, such as height and weight, blood pressure, and cholesterol level. The insurer may also seek an evaluation of blood, urine or oral fluid specimens for underwriting purposes, including tobacco or drug use and HIV infection. Medical tests are done only with the proposed insured's consent. These tests are usually done by a licensed paramedic who typically is employed by a paramedical company. In limited cases, the tests will be performed by a physician in connection with a medical examination requested by the insurer. In either case the applicant will generally be asked to sign another authorization that will contain information concerning HIV and other information relevant to the blood fluid analysis, depending on the state in which the applicant resides and individual laboratory practices. The physician or licensed paramedic may report urinalysis results, record blood pressure and pulse readings, and record comments regarding the proposed insured's condition, including the circulatory, respiratory and nervous systems as well as abdomen, ears, eyes, skin, etc.

The price someone pays for insurance is based on gender, age, the state of health and perhaps job or hobby. Life, disability income, and long term care insurers gather this information about applicants during the underwriting process. Based on this information, a life insurance company groups individuals into pools in order to share the financial risks presented by dying prematurely, becoming disabled or needing long term care. This system of classifying insurance applicants by level of risk is called risk classification. It enables insurers to group together people with similar characteristics and calculate a premium based on that group's level of risk. Those with similar risks pay the same premiums. For example, nonsmokers usually pay less for insurance than smokers. On the other hand, if you have a chronic illness your premium may be higher.

Some individuals are concerned that their medical record information will be "used against them" to deny or cancel coverage, or to increase premiums. In fact, underwriting and the process of risk classification, based in large part on medical record information, have made life, disability income and long term care insurance widely available and affordable: *95 percent of individuals who apply for life insurance are issued policies and 91 percent obtain it at standard or better rates.* Furthermore, *once* a life, disability income, or long term care policy is *issued,* it *cannot be canceled for any reason except for nonpayment* of premiums.

Premiums cannot be raised because an individual files a life, disability income, or long term care insurance claim, or because an individual becomes ill. However, if an individual suffers from a serious medical problem at the time a life insurance policy was issued, the premium could be reduced when the insured individual's health improves. Although some disability income or long term care insurance premiums can go up, this would never happen on an individual basis because of information contained in a medical record. *If* there is a price increase, it has to be on a whole block of policies, usually for economic reasons to ensure that premiums collected are adequate to pay claims.

Once an insurer has an individual's health information, that insurer will limit who sees it. When the underwriting and risk classification processes are complete and the policy has been issued, the medical information in a life, disability income, or long term care insurance file may be accessed and reviewed under certain circumstances. For example, information could be used:

- To process claims for benefits. This information allows insurers to fulfill their contractual obligations to policyholders and pay death, disability income, and long term care benefits. In 1997, more than $ 26.2 billion was paid to beneficiaries under individual life insurance policies.

- By insurance regulatory authorities as part of an examination, or by law enforcement authorities following appropriate legal process who suspect illegal activity, such as murder for insurance.
- If the insurance company is reinsuring a block of business and the reinsurer wishes to review the seller's underwriting practices.
- If the insured applies for additional coverage or seeks to reinstate or change the policy.

THE MEDICAL INFORMATION BUREAU

The Medical Information Bureau (MIB) is a not-for-profit association of life insurers. Its *purpose is to reduce the cost of insurance* by helping insurers detect (and deter) attempts by insurance applicants to conceal or misrepresent facts. As part of the application process, *consumers receive a written notice* which describes MIB and its functions. Furthermore, *member companies will only request information regarding an individual applicant from MIB after the applicant has signed an authorization.*

MIB member companies report to the bureau *brief, coded summaries* of relevant information obtained during underwriting of individuals applying for life, disability income, or long term care insurance. Conditions most commonly reported include height and weight, blood pressure, EKG readings and x-rays if these facts are commonly considered significant to health and longevity. Certain nonlexical information, such as that relating to hazardous activities or adverse driving records, may also be reported, provided such information is confirmed by the applicant or official records. Out of every 100 applications, only 15-20% result in a coded report sent to MIB. *Information relating to amounts of insurance issued, underwriting and claims decisions may not be reported to MIB.*

When a consumer applies to an MIB member company for individual life, disability income, or long term care insurance coverage, the company may ask MIB whether its records contain information on this person. Again, *member insurers may have access to MIB information only after receiving the proposed insured's authorization.* Coded reports from MIB to insurers have two basic functions. The first function is to serve as an alert to detect attempts by applicants to omit or misrepresent facts. The second function is to deter applicants from omitting or misrepresenting significant facts. If an MIB report on the proposed insured does exist, the insurer who receives it will compare the MIB report with information provided by the applicant. If the brief codes in the MIB report are not consistent with other information, the insurer must seek other information about the applicant. *Insurers may not decline an application or charge more for coverage based solely on MIB reports.*

Before accessing MIB records, an insurer must give the individual a notice containing specified information, including *procedures for accessing and correcting information* in accordance with the federal Fair Credit Reporting Act. *Disclosures to individuals or corrections to information are usually done within 30 days.*

The MIB computer system used by member companies for the transmission of this coded information *is exceptionally user unfriendly* to the terminals in its network. MIB uses state of the art technology to verify that MIB reports are properly requested and transmitted. For example, each member terminal has a unique code that identifies that terminal when an inquiry is sent to MIB. The MIB computer will disconnect from the terminal if the identification code is not recognized. In addition, the MIB computer disconnects even after it receives an inquiry presenting the proper identification code. The MIB computer will then dial the company back, using another special code, to establish communication. *All access to MIB is documented.*

MIB recognizes that people who are subjects of reports and public representatives must be satisfied that the MIB system meets legitimate expectations of confidentiality. MIB staff is required to maintain confidentiality under a specified set of procedures, including, among other things: educating all MIB staff as to the expectations of confidentiality; strictly limiting access to the MIB code book and access to the computer room to authorized personnel; and protecting the computer center 24 hours a day with security guards and electronic systems which control access and provide surveillance.

Only authorized personnel at member companies may have access to MIB report information. Reports are not released to nonmember companies or to credit or consumer reporting agencies. MIB member companies must make an annual agreement and pledge to protect confidentiality. The agreement is signed by the president and physician medical director of the member company. Member companies must conduct an annual self-audit to determine whether their procedures have protected the confidentiality of MIB record information. These results must be reported to the

MIB. Member companies must also permit MIB to conduct periodic audits of their confidentiality and underwriting procedures.

THE INDUSTRY'S COMMITMENT

Life, disability income, and long term care insurers have a long history of dealing with highly sensitive personal information, including medical information, in a professional and appropriate manner. Last year, the ACLI Board of Directors adopted a series of Confidentiality of Medical Information Principles of Support. They are attached for your review. The life insurance industry is proud of its record of protecting the confidentiality of this information. Individuals have a legitimate interest in the proper collection and use of medical information about them, and insurers must continue to handle such information in a confidential manner.

The ACLI policy position regarding the importance of protecting personally identifiable medical record information is reflected in our long-standing support of the National Association of Insurance Commissioners (NAIC) Insurance Information and Privacy Protection Model Act (NAIC Model Act). The NAIC Model Act was carefully drafted and tailored to the special information practices involved in the insurance context. The ACLI believes this model strikes a proper balance between the legitimate expectations of consumers concerning the treatment of information that insurers obtain about them, and the need of insurers to use information responsibly for underwriting and claims administration.

The NAIC Model Act governs insurers' practices in relation to all types of information, including medical information. The Act provides consumers with numerous rights and protections in addition to safeguards regarding the confidentiality of medical information. Among other things, it requires provision of a notice of information practices, outlines the content of disclosure authorization forms, imposes limitations and conditions on the disclosure of information and provides a process by which individuals can access, correct, and amend information about them. The NAIC Model Act also outlines remedies for individuals harmed by disclosures made in violation of the Act. Many, if not most, ACLI member companies doing business in at least one state which has enacted the NAIC Model Act adhere to its requirements in all states in which they do business.

LEGISLATIVE PROPOSALS

Several legislative proposals have been introduced during the 106th Congress. We would like to address key issues of concern to the life insurance industry for your consideration as these proposals move forward.

Preemption

As stated previously, we strongly believe that individuals have a legitimate expectation that their health information will be kept confidential. A federal statute that outlines a broadly preemptive set of specific standards to protect this information, and remedies for breach of those standards, will respond to the American public's concern about the confidentiality of their health information. Setting a national, uniform standard for health information, is fundamental to this debate. Consumers would know that they are protected by the same, strong health information privacy law, regardless of their address. Also, life insurance, disability income and long term care companies engaged in business across the country would have a single standard to facilitate the industry's ability to provide financial security to individuals and their families.

Authorization and Revocation

Every year America's life, disability income, and long term care insurers enter into insurance contracts with millions of American consumers. These insurers must utilize health information to evaluate those consumers' applications for coverage and to process their claims for benefits. These contracts can be in effect for decades. In order to prevent federal legislation from inadvertently interfering with the industry's ability to engage in essential, ordinary business functions and to fulfill its contractual obligations, life, disability income and long term care insurers must be able to obtain a *single authorization* for disclosures of information in connection with the ordinary course of insurance business. Such authorizations should not be subject to revocation and should remain valid as long as necessary for the insurer to meet its obligations during the application process and during the lifetime of the policy. Some have suggested that if an individual can revoke his authorization, then the life, disability income or long term care insurance company should have the opportunity to cancel that policy. We urge you to reject this assumption. We cannot cancel our policies. If an individual revokes an authorization, provided in connection with a life, disability income or long term care insurance policy for which he has paid

premiums for thirty years, and the insurer cancels the policy, the individual almost certainly will have trouble replacing that policy—and at what price? If an individual is unhappy with any business practice of the insurer, he always has the right to cancel his policy—he can stop paying premiums.

Right to Self Pay and Scope of Disclosures

In an effort to enhance the confidentiality of some health information, some legislative proposals would grant individuals a right to self pay for treatment they receive and then limit or prohibit the disclosure of health information related to that episode. We are concerned that such provisions could produce conflicting authorizations. For example, assume an individual applies for a life insurance policy and signs an authorization for the disclosure of health information. Pursuant to that authorization, the insurer requests information from a health care provider, however, that health care provider had received *previous instructions* from that individual not to release certain information under a "self pay" arrangement. Which rule applies? The ACLI believes that *all* health information deserves careful, confidential treatment, and that all health information should be treated uniformly.

Language in various bills restricting the "scope of disclosure" to the "minimum amount necessary" is fraught with potential problems. Not only is the legal meaning of "minimum amount necessary" unclear, but the entire philosophy behind this legislation is that individuals should have more control over health information about them. The authorization is the core of the debate. The authorization will govern the scope of a disclosure. Furthermore, we are troubled by some proposals that would have a health care provider determining exactly what is the "minimum amount necessary". A third party would not be in a position to know what information is needed by the entity requesting the information. For example, in the life insurance context, underwriters and medical personnel of the insurer know what information they need to perform risk classification. A provider might not forward information, necessary to the risk classification process, which in his opinion was not necessary.

Damages and Enforcement

As a state regulated industry, we believe that enforcement of federal confidentiality standards applicable to life, disability income, and long term care insurers should be handled at the state level by state insurance commissioners, oversight authorities familiar with the life, disability income, and long term care insurance industries, and their uses of health information. It would be counter productive to create an expensive and unnecessary bureaucracy that would duplicate elaborate and effective systems which already exist in the states.

Bills that have been introduced in this Congress provide for an array of remedies for breaches of health information confidentiality standards. The bills include civil and criminal penalties, and some include a private cause of action. The ACLI strongly objects to punitive damages being provided in a statute. These damages are excessive. The possibility of enormous and unjustified punitive damages is an issue of grave concern to the industry.

Definitions

As with any piece of legislation, the definitions found in medical record confidentiality bills is critical. These words will serve as the foundation and the framework for the new law. At one point during the drafting process in the Senate prior to the Health, Education, Pensions and Labor Committee's markup of the Health Care Personal Information Nondisclosure Act, life insurance benefits were grouped in with health plan benefits and "health plan" was said to include a life insurer. The ACLI encourages this committee to recognize the distinction between lines of insurance, and to maintain those distinctions in the text of the bill. For example, a life insurer is not a health plan; it can be treated as a health plan for purposes of various provisions of the bill, but, again, life insurance is not a health plan.

Applicability

As you know, the entities that would be governed by any federal legislation on health information confidentiality currently obtain, use and redisclose this information. It would be unworkable, and in many instances impossible, to meet the requirements of these bills for information already in the possession of insurers. Accordingly, we strongly urge that a specific section be added to the bill to clarify that the application of these standards is prospective in nature—applicable to health information collected, used and disclosed after the date of enactment.

Other Issues

We would like to work with the committee to ensure that other issues, unique to the life insurance industry and its customers, are addressed as this legislation

moves forward. For example, the law enforcement provisions of some proposals may unintentionally prohibit a life insurer from turning over information to law enforcement authorities where the insurer suspects a murder was committed for the life insurance benefits. Also, beneficiaries must be able to release health information to a life insurer so that they can receive the policy benefits. We welcome the opportunity to work with you, Mr. Chairman and other members of the Subcommittee on these and other important issues as this legislation moves forward.

CONCLUSION

Again, Mr. Chairman, the 493 member companies of the ACLI are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their health information and that insurers have an obligation to assure individuals of the confidentiality of that information. As an industry, life, disability income, and long term care insurers have a long history of dealing with highly sensitive personal information in a professionally appropriate manner. We are proud of our record as custodians of this information.

We welcome the opportunity to assist you in crafting strong legislation to protect the confidentiality of health information and to allow life, disability income, and long term care insurers to continue to serve its millions of customers.

I will be happy to answer any questions.

CONFIDENTIALITY OF MEDICAL INFORMATION

PRINCIPLES OF SUPPORT

Life, disability income, and long-term care insurers have a long history of dealing with highly sensitive personal information, including medical information, in a professional and appropriate manner. The life insurance industry is proud of its record of protecting the confidentiality of this information. The industry is committed to the principles that individuals have a legitimate interest in the proper collection and use of individually identifiable medical information about them and that insurers must continue to handle such information in a confidential manner.

1. Medical information to be collected from third parties for underwriting life, disability income and long-term care insurance coverages should be collected only with the authorization of the individual.
2. In general, any redisclosure of medical information to third parties should only be made with the authorization of the individual.
3. Any redisclosure of medical information made without the individual's authorization should only be made in limited circumstances, such as when required by law in legal proceedings.
4. Upon request, individuals should be entitled to learn of any redisclosures of medical information pertaining to them which may have been made to third parties.
5. All permissible redisclosures should contain only such medical information as was authorized by the individual to be disclosed or which was otherwise permitted or required by law to be disclosed. Similarly, the recipient of the medical information should generally be prohibited from making further redisclosures without the authorization of the individual.
6. Upon request, individuals should be entitled to have access and correction rights regarding medical information collected about them from third parties in connection with any application they make for life, disability income or long-term care insurance coverage.
7. Individuals should be entitled to receive, upon request, a notice which describes the insurer's medical information confidentiality practices.
8. Insurance companies providing life, disability income and long-term care coverages should document their medical information confidentiality policies and adopt internal operating procedures to restrict access to medical information to only those who are aware of these internal policies and who have a legitimate business reason to have access to such information.
9. If an insurer improperly discloses medical information about an individual, it could be subject to a civil action for actual damages in a court of law.
10. Any federal legislation to implement the foregoing principles should preempt all other state requirements.

Mr. BURR. We thank you, Ms. Meyer. I think you had a little extra time. I think our clock is—I can assure all of you that we do understand the severity of what we are charged to do. I think I can

only speak for this committee. I think we will try to do our best at it.

We certainly appreciate, especially you, Mr. O'Keefe and Ms. Meyer, for coming to this hearing room versus the one downstairs because I am sure you are just as concerned with what is coming out of the banking bill as it relates to insurance.

Let me recognize myself for 5 minutes and turn to the good doctor over here and just ask you, how would the flow of electronic claims at Envoy be affected or in any other companies for that fact, if you had to comply with 50 different sets of regulatory bodies out there?

Mr. ZUBELDIA. Because of the complexity of those potential differences, some of the claims would have to go on paper. Some of the eligibility inquiries could not be handled electronically. It would have to be handled by telephone.

A few years ago, we had an experience with one of the States that required that their Medicaid claims be signed, and that was a State requirement way back from when they instituted the Medicaid program. They never considered the possibility of having an electronic signature, and in that State all the Medicaid claims were going on paper.

We could revert back to a scenario like that in which maybe mental health claims would have to go on paper or cancer claims or any claim with a diagnosis that could suggest cancer or mental health or certain diagnosis groups would have to go on paper because of the impossibility of handling electronically without the patient's consent.

And we believe that handling these transactions on paper exposes them to a much greater risk than electronic transactions which are for the majority, maybe 80 percent or more, adjudicated without a human hand or anybody seeing them. They are adjudicated by a machine. So by moving to a paper flow, we are not gaining anything, and we are getting into a high risk area.

Mr. BURR. Let me go to you, Ms. Koyanagi. You referenced in your statement that there were certain groups that could be identified where privacy is a very key issue, and I think we probably all know the meat of that list. And I think you sort of answered the question of preemption much like Dr. Hamburg did. I call it a modified preemption, but I am not yet convinced nor do I have a firm opinion one way or the other.

I am not yet convinced you can do that. Under a modified preemption, though, let's assume that we could come up and we could craft something that the balance was there. Aren't you still concerned that you have got these 50 individual pieces of patchwork that still won't accomplish the confidence level for certain groups to feel comfortable with the privacy laws?

Ms. KOYANAGI. Well, I think I would like to say two or three things about that. The first is if you enact a Federal floor, hopefully, that provides a level of confidence. If your floor is so low that it doesn't, then I think you, hopefully, will revisit it. The confidence across the country can come if there is some significant privacy protection in the Federal floor.

Second, I think one could always come up with a lot of hypotheticals about what 50 States might do. It is important to see,

I think, what they really do with the enactment of a Federal bill that would put in place a set of privacy protections that will probably be stronger than most of what the States have already so that, in fact, you are likely to see as, I said earlier, very few provisions in very few States that go beyond the Federal statute.

Right now the companies deal with 50 State laws, and they are managing to do it. I doubt that too many States will go back and revisit whether the records should be on paper or not. Maybe they will. But there is nothing to prevent the Federal Government giving them the opportunity to show that, in fact, they can behave very responsibly and, in fact, deal with their local situations without creating chaos. If you don't like what they have done, you can come back in a year or 2 and preempt, not close the door.

Mr. BURR. Given that the States—you referred to the States having moved because of the lack of any Federal statute. Given that the States have moved and understanding that this is really a response to the technological advances that exist, is there any confidence that you have that current State statutes are more apt to change to reflect the technological changes?

One of the concerns that I have is when the Federal Government sets a floor or preempts, and I think yours is a floor that is much closer to the ceiling than possibly where I envision one, but that becomes a target that is hard to move because it has to go back through this legislative process up here. What is your level of confidence that States, as they see this advance in technology in the absence of a Federal initiative that preempts, would adjust their State statutes to reflect the change in technologies?

Is there any belief in your part that that would happen?

Ms. KOYANAGI. I think it is slowly happening, and I think you would see, as usual with the States, that some would move more rapidly than the others and some may never act.

You would get different reactions in different places, but I think with the publication of certain proposed model State statutes on privacy, we will begin to see if the Federal Government does not act, that the States will step in.

Mr. BURR. Is there any reason for us to err on the side of the floor being slightly lower than slightly higher as we try to find that balance?

Ms. KOYANAGI. I would go back to my first point which is the protection of patients needs to be a major priority here and patient confidence in the health care system.

I don't think most people have a clue really how their information gets out to how many people it gets out. Think of places such as rural areas where everyone knows everyone, and it is rather easy to find out this kind of information. All kinds of consequences can come from that and will come from that. And we will get stories in the papers like we had recently where a drug company sent records to—a pharmaceutical drugstore sent records to a company.

Mr. BURR. I think we actually entered into the record a clarification by the Washington Post that that did not happen, that the drug—the pharmacy had contractual agreement that the mailhouse could not and did not distribute to the pharmaceutical company the name of those patients.

I would tell you that my concern—initial concern on the rule side is exactly the opposite, the difficulty with accessing the people. Montana might be a great example. The people don't live exactly that close together and certainly one of the problems that we have in rural North Carolina with the delivery of health care is identifying the individuals that need it. It is not with this overwhelming flow of them coming in or with a shared access of information. It is with the inability to disseminate the information. It is not personal records, though.

With the ranking member's indulgence, let me just ask Ms. Meyer one question, if I could. Your testimony said, and I quote, setting a national uniform standard for health information is fundamental to this debate. That along with what you said verbally is supportive of a preemption of State law; am I correct?

Ms. MEYER. Yes, it is.

Mr. BURR. Thank you.

The Chair would recognize the ranking member.

Mr. BROWN. Thank you, Mr. Chairman.

Mr. O'Keefe, welcome. If you were—if we here were not successful in passing privacy legislation, could you tell us what U.S. interests might be hurt by the EU regulation that you showed?

Mr. O'KEEFE. Mr. Chairman, Congressman, you know, I feared you might ask that, and I was thankful when it came up a little bit earlier.

I will answer to the best of my knowledge, but the first time I saw this was yesterday. It is my understanding that should commerce fail to negotiate a set of agreements on privacy with the European Union, then any company doing business in the insurance industry, for instance, in the medical research areas, in pharmaceuticals, could—their product could be at risk or their cooperation with European companies could be at risk because of the protection of the Europeans involved in either the research, the insurance products, and/or the medical treatment would not be protected.

Now, I am not sure and I am sure that staff at NAIC could research that more fully and provide you with that information.

Mr. BROWN. I would like that. Certainly none of us is able to predict, but would there be a trade action, WTO trade action filed against—by the EU against us, against the United States, or would the U.S. file a trade action in front of the WTO and perhaps on—against the EU on what that would do to the American biotech or pharmaceutical industries? If you would—if NAIC could research that——

Mr. O'KEEFE. We will supply that. As I told staff this morning, the only thing Montanans know about Europe are the agreements having to do with wheat. So we will make sure that staff gets that to you immediately.

Mr. BROWN. Thank you. Speaking of the NAIC, tell us, you mentioned more sort of from Montana's viewpoint and Montana's constitution about confidentiality. Talk through, if you would, why it is important for NAIC to have a floor understanding. Ms. Meyer representing the trade association for insurance took the opposite position.

Mr. O'KEEFE. Well, Mr. Chairman, Congressman Brown, I think that one thing that is interesting about NAIC is that we realize the

diversity amongst the 50 States and the different needs in each State and in each marketplace and the way the States historically have responded to that.

One of our major concerns is that there are States like Montana where—and it is my understanding that we are the only State in the last 8 months to pass a comprehensive privacy of medical records act aimed at the insurance industry during our State legislature, and we have been very, very aggressive about that.

Last fall a model act was passed by NAIC in September, and each State is considering that. We think that a floor is necessary because anything less than a floor, you run the risk of taking away protections from citizens that are already in place. And we think that is a dangerous thing to do.

In Montana or Minnesota, the protections may be very high while in other States they may be very low. I think your goal is to have a minimum standard that protects the individual's medical records. I don't think your goal is to take protections away from individuals that work in the current system. And in Montana, for instance, while our level is very high, the bill that I led through the legislature was signed off on by consumers, by medical researchers, by insurers, and by regulators, so we were able to do it in a way where all of those needs were met.

A floor should do that; and if any State sees the need to get additional protections, they should have the right.

Mr. BROWN. Could I have an additional couple of minutes? Thank you.

Thank you, Mr. O'Keefe. Ms. Koyanagi, your testimony, written and oral and others, have indicated that mental health patients are, putting it mildly, not especially comfortable with existing privacy protections.

Discuss with the subcommittee, if you would, how these protections or lack of protections affect consumers in their decisions to seek mental health care?

Ms. KOYANAGI. There have been studies of that. If you want it, I can provide something for the record. The behaviors that I was describing in terms of the California poll, which was taken of all consumers, are very prevalent in terms of people seeking mental health care. A lot of times people will not come in for treatment. The consequences of the stigma around mental illness, concern that that information may get back to their employer, people have lost their mortgages, people have lost their jobs, people have lost their insurance as a result of mental health utilization becoming known. Those may not be legal behaviors but they do occur. So they are just very, very scared of that and so they don't seek treatment, they delay treatment or they don't provide all the information. They go to someone who hasn't done their physical health care so there is no coordination of care because they are trying to keep the mental health care very private. So it has all kinds of consequences and that has been studied.

Mr. BROWN. And they are worried about what they actually say to their mental health professional also.

Ms. KOYANAGI. Absolutely.

Mr. BROWN. There is physical health—it is their physician of their physical health, their mental health counselor, physician pro-

vider, and it is just a question of many—you assert many people do not even seek any kind of care because of fears of privacy.

Ms. KOYANAGI. Right. Those who can afford it may private pay, but for many of us that would not be feasible.

Mr. BROWN. That is all I have, Mr. Chairman. Thank you.

Mr. BURR. Let me take this opportunity just to thank these witnesses and to suggest to you if it seems like sometimes we ask questions from both ends of the issue, we do. We are desperately trying to figure this out.

I would also comment that I think I have heard floor defined as about eight different things today and all of them are right. And we realize that. And part of this process is to make sure that as we go through that, we can, with confidence, say to that mental health patient or to that AIDS patient or to any patient out there, your records are secure; and to the health care providers that we have done something that has not driven health care to a point where nobody can afford it; and to the pharmaceutical companies that our great efforts at actual cures for terminal illness can continue and continue with the optimism and prosperity that we have seen; and that for all who need access to medical records with the approval of patients that that is available.

Clearly we understand we have a very difficult job, but I don't think that this committee will pass on this responsibility.

I want to thank you one last time. This hearing is adjourned.

[Whereupon, at 2:35 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF THE ASSISTANT SECRETARY FOR PLANNING AND EVALUATION
Washington, D.C. 20201

Ms. KAREN FOLK
Committee on Commerce
564 Ford House Office Building
Washington, D.C. 20515

DEAR MS. FOLK, enclosed are the responses to the questions for the record from the May 27 hearing on Medical Records Confidentiality. I apologize for the delay in providing this information.

Please contact me if you have any further questions.

Sincerely,

MARGARET A. HAMBURG, M.D.
Assistant Secretary for Planning and Evaluation

QUESTION FROM REP. JOHN D. DINGELL

Question 1. Could you elaborate on the enforcement provisions in the Secretary's recommendations and explain why they should be included in any privacy legislation? In particular, could you explain what you mean by a private right of action and why it is important to give individuals recourse for violations of their privacy protections?

Answer: We need to send the message that protecting the confidentiality of medical information is vitally important, and that people who violate that confidence will be held accountable. There should be punishment for those who misuse personal health information and redress for people who are harmed by its misuse.

Federal legislation should include criminal felony penalties for obtaining health information under false pretenses, and for knowingly obtaining or using health information in violation of federal nondisclosure requirements. Penalties should be higher when violations are for monetary gain. Legislation should also provide for the assessment of civil money penalties against any entity that demonstrates a pattern or practice of unauthorized disclosures.

In addition, any individual whose rights under a federal privacy law have been violated should be permitted to bring an action for damages and equitable relief. It is critical that federal legislation provide individuals with the ability to seek redress.

We have seen the standards set in some legislation set so high that it would effectively bar an individual's ability to bring a suit. We are willing to work with you to ensure that it is set at an appropriate level.

QUESTIONS FROM REP. HENRY A. WAXMAN

Question 1. Do you believe that strong federal protections relating to individually identifiable health information would increase uniformity among state laws? Please explain the rationale for your position on this matter.

Answer: If the Federal legislation is strong enough, then the States may not feel the need to enact stronger laws. We can go a long way to creating uniformity by enacting legislation with a strong federal floor. For example, we have had this experience since the passage of HIPAA—States are allowed to pass laws that extend beyond the Federal floor of HIPAA, but they generally have not done so.

Question 2. Do you think it is a wise policy to ensure that states have the flexibility to enact heightened privacy protections for health information to address issues that may be of particular concern to states? Please explain the rationale for your position on this matter.

Answer: The Administration's general view is that federal statutes which establish new health protections for individuals should set a floor upon which states can build to address their unique circumstances. A federal privacy law should create a minimum standard, a minimum assurance of privacy on which the public can rely. But, it is important to preserve State options to respond to new medical privacy challenges. The federal government cannot anticipate future needs and developments in the health care industry, nor can we effectively respond to the unique demands of some State systems. Therefore, it is critical that we enact strong federal protections and at the same time, preserve State options and flexibility for the future.

Question 3. Do you believe that the review process for health research disclosures set forth in the recommendations is practicable? Please explain your rationale for this position.

Answer: Today, the Common Rule and FDA's Human Subject Regulations protect participants in most research studies that are funded or regulated by the federal government. We recommend that similar protections be extended to all research using individually identifiable health information, not just federal research. It is our position that there should always be some type of review mechanism for researchers who wish to use medical records without obtaining a patient's prior authorization, regardless of their funding source. Such a review mechanism should operate under principles like those in the Common Rule, and must have some accountability.

Based on our experience with the Common Rule and IRBs, we believe that this type of review process is workable for privately-funded research. NIH and other federal agencies follow requirements similar to those outlined in the recommendations, and there is no lack of people looking for federal funding for their research. A review process should increase people's confidence that the privacy of their information will be protected, and increase their willingness to participate.

Question 4. Why do you believe that it is important to ensure privacy protections for health information?

Answer: The existing legal structure does not effectively control information about individuals' health. Federal legislation, establishing a basic national standard of confidentiality, is necessary to provide rights for patients and define responsibilities for record keepers.

There are certainly numerous examples of serious violations of the privacy of our medical records. We have heard about an HMO that allowed every single clinical employee to tap into patients' computer records and see detailed notes from psychotherapy sessions, about a medical student who copied and sold health records to medical malpractice attorneys, and a newspaper that published information about a congressional candidate's attempted suicide. The new owner of a used computer that originally belonged to a pharmacy found detailed patient records still on the hard drive.

But the more important point is that the ways we use and share medical information are changing. Today, almost 75 percent of our citizens say 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 vital information to their doctors, getting needed treatment or seeking genetic testing. Such distrust, if left unchecked, can undermine progress in our entire health care system.