S. HRG. 104–320

MEDICAL RECORDS CONFIDENTIALITY ACT OF 1995

HEARING

OF THE

COMMITTEE ON LABOR AND HUMAN RESOURCES UNITED STATES SENATE

ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

ON

S. 1360

TO ENSURE PERSONAL PRIVACY WITH RESPECT TO MEDICAL RECORDS AND HEALTH CARE-RELATED INFORMATION, AND FOR OTHER PURPOSES

NOVEMBER 14, 1995

Printed for the use of the Committee on Labor and Human Resources

U.S. GOVERNMENT PRINTING OFFICE
21–015 CC WASHINGTON : 1996

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-052250-1

COMMITTEE ON LABOR AND HUMAN RESOURCES

NANCY LANDON KASSEBAUM, Kansas, *Chairman*

JAMES M. JEFFORDS, Vermont
DAN COATS, Indiana
JUDD GREGG, New Hampshire
BILL FRIST, Tennessee
MIKE DeWINE, Ohio
JOHN ASHCROFT, Miasouri
SPENCER ABRAHAM, Michigan
SLADE GORTON, Washington

EDWARD M. KENNEDY, Massachusetts
CLAIBORNE PELL, Rhode Island
CHRISTOPHER J. DODD, Connecticut
PAUL SIMON, Illinois
TOM HARKIN, Iowa
BARBARA A. MIKULSKI, Maryland
PAUL WELLSTONE, Minnesota

SUSAN K. HATTAN, *Staff Director*
NICK LITTLEFIELD, *Minority Staff Director and Chief Counsel*

CONTENTS

STATEMENTS

TUESDAY, NOVEMBER 14, 1995

APPENDIX

MEDICAL RECORDS CONFIDENTIALITY ACT OF 1995

TUESDAY, NOVEMBER 14, 1995

U.S. SENATE,
COMMITTEE ON LABOR AND HUMAN RESOURCES,
Washington, DC.

The committee met, pursuant to notice, at 9:30 a.m., in room SD–430, Dirksen Senate Office Building, Senators Kassebaum (chairman of the committee) presiding.

Present: Senators Kassebaum, Jeffords, Gorton, Kennedy Simon, and Wellstone.

OPENING STATEMENT OF SENATOR KASSEBAUM

The CHAIRMAN. This morning's hearing will please come to order.

I would like to welcome everyone, perhaps because this is just a rather warm and sheltering place at this point, to this morning's hearing on S. 1360, which is the Medical Records Confidentiality Act of 1995.

Much time has been spent the last several months, and the author of this legislation, Senator Bennett, has been the chairman of the Republican Task Force on Health Care Issues. We have spent a lot of time debating health care issues, from health insurance reform, of course, to Medicaid and Medicare proposals which are in the reconciliation legislation.

And as we debate these changes, the private health care system continues to change literally overnight as it adjusts to all of the different forces that are at work. And while health providers still wrestle with multiple paper forms and bulky files, increasingly, health information and data are digitally transmitted to multiple database by highspeed computers over fiberoptic networks.

Since 1988, the percentage of health claims processed electronically has grown from only 8 percent to nearly 40 percent today. Many Americans believe their private medical records are safely stored in doctors' offices and hospitals; yet the evolving health care delivery system and the advanced technology necessary to support it has left gaping holes in the patchwork of current State privacy laws and threatens the confidentiality of private medical information.

Examples today will highlight both the promise and the peril of the medical information, and I look forward to hearing from the witnesses who will provide those examples.

I believe the Medical Records Confidentiality Act takes a balanced approach to encouraging the continued development of a

world-class health information infrastructure, while at the same time assuring all Americans that their sensitive medical records are protected.

I certainly applaud Senators Bennett and Leahy for taking on such a complex and important issue. It has been debated on and off for a couple of years, and we have never been able to quite get the right balance. This has been an issue of concern to both Senators, and I look forward to working with them and with my colleagues on this committee to see that this important piece of legislation is enacted in the 104th Congress. So I look forward to today's hearing.

Senator Kennedy has urged us to go ahead with the hearing; he will be here a bit late. Senator Leahy is also running a bit late.

The CHAIRMAN. I would like to introduce someone whom I know has thought a lot about this, has spent a great deal of time and is concerned about this issue. It is a pleasure to welcome our colleague, Senator Robert Bennett, who introduced the Medical Records Confidentiality Act.

Thank you for being here, Bob.

STATEMENT OF HON. ROBERT BENNETT, A UNITED STATES SENATOR FROM UTAH

Senator BENNETT. Thank you, Madam Chairman. I appreciate the opportunity to be here, and I want to thank you not only for holding the hearing, but for your acknowledgment of the importance and significance of this legislation.

I am pleased that Senator Leahy was planning to be with me, and I am sure he is with us here in spirit, because of his great involvement in this issue over the years. It was a sense of some comfort to me that when we introduced the bill, Senator Leahy was one of the first to come forward and say he would like to serve as a cosponsor.

I would like to note for the record that both the chairman and the ranking minority member, Senator Kennedy, are cosponsors of the legislation, as is the Majority Leader, Senator Dole, and the Democratic Leader, Senator Daschle. And I am very appreciative of that kind of support going in.

There are few areas in our lives that are more personal and private than our medical histories. We have relationships with doctors, nurses, pharmacists, and other health care professionals that is unique and privileged. They may know things about us that we choose not to tell our spouses or our children or siblings or parents, even our closest friends, at times. Our medical records may contain nothing out-of-the-ordinary, but these records are of the highest private nature, and I believe we have the right to expect that they will be handled with dignity and caution and care.

Many Americans believe that medical records are protected in this manner right now, but they are mistaken. The expectation is not guaranteed as a right.

I have brought along several charts that illustrate the patchwork of difference that exists now, with this issue being controlled by State law. This first chart shows that confidentiality laws exist in 34 States, those in yellow, leaving those in gray without such legislation, one of which is my home State of Utah.

The CHAIRMAN. And mine as well.

Senator BENNETT. Kansas as well.

The health care professionals in Utah have contacted me and said, "But Senator, you are implying that things are terrible in Utah, and in fact things are going rather well in Utah," and they cite a series of practices which are salutary, that health care professionals have voluntarily adopted. That is wonderful, but the fact that they have been voluntarily adopted indicates that they can be breached by those who choose not to follow them, without any consequence or sanction.

The second chart shows those States that allow you access to your medical records. There are only 28 States that do. The States in red provide access to hospital and physician records, again with differing procedures from State to State. The States that are crosshatched in the red and white show hospital records only, and in the States in yellow, there is no formal requirement that a patient have access to his records.

Ironically, Madam Chairman, you have more right to see your credit report and make corrections to records dealing with your money than you do your medical report in those States that are shown in yellow.

It is time to put into place the safeguards and security measures needed to protect the integrity and confidentiality of medical records, and patients should be assured that the treatment they receive is a matter between themselves and their doctor, regardless of whether it is a yearly physical or a psychiatric evaluation, plastic surgery, or cancer treatment.

S. 1360 is an opportunity for the Congress to act in a bipartisan manner to resolve this important problem.

Most people agree that the legislation is important, but many disagree on how it should be brought to pass, which is why this has not produced a solution in the years that it has been studied.

Prior to introducing the bill, my staff, working with those of other Senators who have served as cosponsors have put forward months of work, and many organizations supporting various interests have come together to formulate what we think is a workable solution for securing medical records privacy. We have tried to work with patients' rights advocates, with computer experts, with hospital organizations, medical organizations, people all across the spectrum. It has been very interesting, however, that after we introduced the bill, a number of other people came forward to say, "Wait a minute—we did not know you were working on this, and if we had, we would have suggested," and so on.

In every case, I have said to these folks that is what hearings are for and urged them to make their representations to this committee, and I am sure the committee will be thoughtful in examining the various suggestions that have come to us. I said once we have introduced the bill, the drafting process is out of our hands and passes to the committee and the amending process.

Now, Madam Chairman, the purpose of the legislation, as you well know, is twofold—first, to provide Americans with greater control over their medical records in terms of confidentiality, access and security. Most patients are unaware that their records are accessible to almost any health care provider walking into the room,

or almost any hospital employee with a computer who can gain access to the hospital's computer system.

We found as we went through the drafting process that a number of doctors and nurses routinely refuse to be treated in hospitals where they practice because they know that their fellow employees, with the stroke of a computer key, can find out everything about them, and so they prefer to go to other hospitals simply to maintain confidentiality among their fellow workers. That demonstrates to me as dramatically as anything can how serious a problem this is. When those who are the closest to the system understand its failings and refuse to seek treatment in the very places where they work, it sends a strong signal.

Not only do patients have limited control over who has access to their medical records; in many instances, they have the most difficulty gaining access to their own records. As I said, Madam Chairman, they have an easier time getting into their credit reporting than they do their medical reporting. And there are no Federal laws concerning personal access. As this chart shows, a patchwork of State laws allowing people access to review and copy their medical records. So that if there is an error in your medical record that you know about, in those States shown in yellow, you do not have a legal right to correct that error, and it can follow you from place to place.

The legislation proposed here today provides a means through which patients may review and correct personal medical records, and it gives the patients the right to limit disclosure of their medical records for purposes other than treatment and billing.

The second purpose of the legislation is to provide the health care system with a Federal standard for handling identifiable health information. One of the interesting things that I found out as we got into this process was that at the moment, roughly 50 percent of the United States population lives on the State border. It is very likely that they live in one State and go to a hospital or a doctor who lives in another State. In this metropolitan area, we live on three State borders. One could live in Virginia, see a doctor in Maryland, and be referred to a hospital in the District.

This cries out for a Federal standard handling this vital information and the patchwork of State laws that these charts demonstrate show how difficult it would be. S. 1360 will provide the organizations and entities involved in providing health care, or those who are contractor or agent to providers, to abide by a single national standard for confidentiality. Thus, having one standard will not only simplify the business of health care; I think in the long run it will reduce the cost of health care, because no longer will people have to comply with differing standards for those 50 percent of our population that live on the State line.

For that reason, Mr. Chairman, I have put forward the legislation. As I said at the beginning of the statement and will say now that Senator Kennedy has arrived, how grateful I am for the bipartisan support that has surrounded this issue, and I hope this can move forward now without the contention that sometimes surrounds health care issues, because this is something that we can handle without searing ideological differences, and I think it is an issue that we need to move forward on as quickly as we can.

The CHAIRMAN. Thank you very much, Senator Bennett. I appreciate those thoughtful comments.

Senator Kennedy?

OPENING STATEMENT OF SENATOR KENNEDY

Senator KENNEDY. Thank you, Madam Chairman.

I will put a statement in the record, but I want to thank Senator Bennett and Senator Leahy. An immense amount of work has gone into this legislation. The issue of privacy is essential, and lacking today in too many instances. This represents, I think, an enormously constructive and positive product. Different items have been raised, and obviously, we want to hear the recommendations and suggestions that will come forward, but I want to thank Senator Bennett and Senator Leahy. Senator Leahy worked with us a year or so ago when we were looking at a more comprehensive health care program, and many of these matters were brought forward and thought a good deal about.

I thank Senator Bennett. I remember talking with him a few months ago about some of the different recommendations in the health care area, and he has done a lot of work on this, so I welcome the fact that Senator Bennett is a prime leader in this area, and he is also a cosponsor of the Kassebaum bill on the preexisting condition legislation, which I am hopeful we can pass in a bipartisan way as well, which is incredibly important, and I take my hat off to our chair, Senator Kassebaum, for her leadership in both of these areas, and I join with Senator Bennett in hoping that when we get these other little, minor issues resolved that are out there, we can get to some things which will have an important impact on people's lives.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you, Senator Kennedy.

[The prepared statement of Senator Kennedy follows:]

PREPARED STATEMENT OF SENATOR KENNEDY

I commend the distinguished Chair of the Labor and Human Resources Committee, Senator Kassebaum, for holding hearings this morning on the Medical Records Confidentiality Act of 1995. Protecting the confidentiality of personal and sensitive medical information is vital as we work to develop an integrated, accessible, cost-effective and quality health care system for all Americans. I thank also Senator Bennett and Senator Leahy for introducing this bipartisan bill. I know they have worked diligently with health care providers, health information specialists, legal experts and consumer groups to balance a wide variety of interests and concerns. I look forward to hearing their testimony this morning.

This hearing builds upon the work already done on the bill and will clarify the issues that remain. We all share the goal of protecting privacy while providing high-quality health care. I supported the Leahy amendment to the Health Security Act last year and I support this bill now. I hope that we can make it stronger and deal effectively with the remaining concerns. We need to work together to develop effective ways to keep medical information safe, secure, and confidential. At the same time, we must take advantage of the

cost-savings and other benefits associated with electronic maintenance and transfer of medical information.

The current state of federal and state law is inadequate. The small patchwork of federal law does not prohibit collecting, sharing, and selling private medical information. Only 28 states guarantee access by patients to their own medical records. Only 34 states have any level of privacy protection.

Too often, current legal standards depend on the type of information collected and the purpose for which it is used. The variations in state law and the weaknesses in federal law clearly demonstrate the need for federal standards in the face of the growing accessibility of private information on medical records.

The pending bill puts necessary restrictions on access to medical information by requiring patient authorization for release of the information. Pharmaceutical companies should not be able to buy a patient list from an insurance company or an HMO in order to market a new drug. Employers should not be able to obtain personal medical information in administering a company's health plan. Patients should have a right to see and correct their records.

We also need to assess the claims of law enforcement officials and health researchers for access to private records, and a major purpose of this hearing is to address these concerns. Clearly, the burden of proof should be on those who feel that exceptions to privacy are needed.

I look forward to the testimony of our witnesses today, and to working with my colleagues to fashion effective legislation.

The CHAIRMAN. Senator Gorton, do you have any opening comments you wish to make?

Senator GORTON. No, Madam Chairman.

The CHAIRMAN. Senator Simon?

Senator SIMON. I simply want to join Senator Kennedy in commending you, Madam Chair, and Senator Bennett for your leadership on this. I think that one of the things that people are discouraged about in Congress is our inability to work together across party lines, and we have some dramatic illustrations of that today; but here is an example of where something constructive can happen. And let me just add that it is my observation that Senator Bennett, still a relatively new Member of the Senate, is not frightened by a new idea. I think that is very important for a Member of the U.S. Senate.

I regret that I am going to have to go to another hearing, but I really appreciate the contribution Senator Bennett has made here.

The CHAIRMAN. Thank you very much.

While we are waiting for Senator Leahy, maybe I could start by asking a couple of questions. I would be curious, was there any particular case that happened in Utah or somewhere else that sparked your particular interest in devoting the time and energy that you to trying to pull together what has been a very contentious issue?

Senator BENNETT. Not really, Madam Chairman. When I became the chair of the Republican Health Care Task Force, at our first meeting, I said to my colleagues, "Let us not discuss any proposals for health care reform for the 104th Congress at this first meeting.

Let us spend this meeting reviewing the efforts that went into this issue in the 103rd Congress and see if there are any lessons we can learn from what happened or, more accurately, did not happen in the 103rd Congress with respect to health care reform."

As we talked through that experience, we realized that a very fundamental political mistake was made by trying to offer an omnibus will that would wrap together all aspects of health care in a single piece of legislation. What happened in my view was that you ended up with the enemies of Section 1 becoming the enemies of the entire bill; the enemies of Section 2, a different set of enemies, becoming the enemies of the entire bill; the enemies of Section 3, a still different set of enemies, becoming enemies of the entire bill, and so on. So that the omnibus bill ended up with so much opposition that it ultimately died.

And we decided in that first meeting that if there were a way we could break out certain aspects of health care reform that might not attract so many enemies that they could not pass and offer them as individual bills—that is what you have done, Madam Chairman, in your insurance reform bill dealing with preexisting conditions. Virtually everyone in the health care debate recognized that that is a reform that was necessary. The fact that you were able to craft a bill on that issue and report it out of this committee unanimously demonstrates the wisdom of that approach.

So, as we sifted through all of the aspects of health care reform, we came across this one and realized that it, too, was something that had been in everybody's bill. It was in President Clinton's proposal, it was in Senator Mitchell's bill, it was in Senator Chafee's proposal; it was in virtually everyone's proposal. And at that point, I thought, well, then, why don't we pull it out and see if we can't produce a bill on this subject alone, and that was the impetus, rather than a particular horror story, that got us started.

The CHAIRMAN. Since it has been out and discussed some, and you have heard from constituencies and groups who have looked at it, do you have any suggestions for changes that could be considered?

Senator BENNETT. I do not have any specific suggestions to offer because the reactions have been more general than specific. The one area that has stimulated the most comment is the possibility of computer banks being formed on the medical information that might produce a "big brother" effect—that is, where people who have access to the computer banks might be able to track medical histories along with credit histories by matching Social Security numbers, and thus create some kind of super-Government surveillance. If this sounds a little like the mentality that accompanies those who were trying to justify the Oklahoma City bombing, that I think would be stretching things—that is, the fear that the Government, with black helicopters and computer banks, is somehow going to track every aspect of our lives.

Nonetheless, I think it does raise a legitimate issue about confidentiality and what happens as records are added to large pools that the committee ought to look at. I have asked everyone who has raised this issue with me, Do you have any specifics other than the general concern, and so far, the answer has been no; but we

are trying to find some specifics and alert the committee. You will hear from people on that.

Senator KENNEDY. If the Senator would yield—the fact of the matter is that it is already happening, isn't it, without these protections? I think that is one of the very commendable parts of your bill. That is already happening without these protections. Maybe they do not know about it and they will focus in on that element of it in terms of the legislation, but I think this ought to be a matter of continuing concern that that is the case today and is going on with great rapidity with all of the information-based systems.

I often cite the example that my son had cancer, and if he was tested in Boston in the morning for insurance and then went out to California that afternoon and went into an insurance company, they would all have his complete information out there. So that is already happening industry-wide, and there is also this collection of material. So they ought to understand that this is an additional kind of protection.

But I think your point is well-taken that we have to be able to make that case, and I think it is important that we do that, and I think we need suggestions as to how to make sure the protections are there.

Could I ask one final question?

The CHAIRMAN. Please.

Senator KENNEDY. One of the exemptions deals with information available to the security police, and we use the standard of the preponderance of evidence. I am not interested today in getting into what that standard ought to be, whether it is preponderance or some other kind of a test. I suppose this might be an area that we can look at. I think some of the enforcement agencies have talked with us about what that standard should be, and I imagine you would be open to seeing how we can work out way through that.

Senator BENNETT. Absolutely, Senator. The law enforcement people with whom we talked as we went through the drafting process expressed some concern about the bill's stress on confidentiality getting in their way as they used medical reports for identification purposes and seeking fugitives from justice. So our intent in the way the language was written was to try to preserve existing law enforcement rights, not expand them. And if in fact we have done something that would create a "big brother" effect in that area, we are more than willing—speaking for the staff, I am sure, who worked with me and the other organizations that worked with us—to accept amendments in that area.

Our intent was to preserve existing law enforcement opportunities, and we hope we have done that.

Senator KENNEDY. Thank you, Madam Chairman.

The CHAIRMAN. Are there any other questions for Senator Bennett?

Senator KENNEDY. I think you have preserved as well the States' roles in some areas, as well, have you not, to permit them in certain areas of activity to be able to have stronger legislation?

Senator BENNETT. Yes, but we are striving for a single Federal standard for the reasons that I outlined in my opening statement, so that practitioners will not be forced to keep two sets of records if indeed their patients are across State lines. But we recognize

that there are State roles, and to the degree we can accommodate that within the overall goal, we have tried to do that.

The CHAIRMAN. Thank you very much.

Let me just say that Senator Leahy is still at a meeting at the CIA, so I think we will go ahead. He has asked us to do so and will stop by if and when he gets back.

I would like to invite you, Senator Bennett, to join us if you have time, for as long as you can.

Senator BENNETT. Thank you.

The CHAIRMAN. It is a pleasure now to introduce the second panel and to welcome Dr. Don Detmer, who is a university professor of health policy and surgery and vice president-provost for health sciences at the University of Virginia in Charlottesville. Dr. Detmer currently chairs the Institute of Medicine Board on Health Care and Services and has long been interested in this subject. It is a real pleasure to welcome you today.

Jeanne Schulte Scott is director of government and legal affairs for CSI Technologies, a Tulsa, Oklahoma-based health claims clearinghouse.

I think Senator Jeffords will be coming, so I am going to skip you, Ms. Roberts, because he would like to introduce you since you are a Vermonter.

Next, I will introduce Kathleen Frawley, who is director of the Washington, DC office of American Health Information Management Association. Prior to joining AHIMA, Ms. Frawley was vice president and counsel for the Jamaica Hospital Center in New York City. It is a pleasure to welcome you this morning.

Since Jeffords has not yet arrived, perhaps I will go ahead and introduce Ms. Roberts.

Senator KENNEDY. Well, as a fellow New Englander, we are delighted to have you here.

The CHAIRMAN. That is right. [Laughter.]

Senator KENNEDY. I know Senator Jeffords can do a lot better than that.

The CHAIRMAN. Yes, and I am sure he will reintroduce you when he comes, but let me just say it is a great pleasure to welcome you here, and we will go ahead and start the testimony with Dr. Detmer.

Let me just say also that there have been a number who wished to testify this morning, and I appreciate all of those who have an interest in this hearing, and if anyone has been inconvenienced, we apologize. But all the statements of those who have submitted testimony will be made a part of the record, and of course, for all those testifying, their full statements will be made a part of the record.

Dr. Detmer.

STATEMENTS OF DR. DONALD E. DETMER, UNIVERSITY OF VIRGINIA, CHARLOTTESVILLE, VA; JEANNE SCHULTE SCOTT, CSI TECHNOLOGIES, McLEAN, VA; CAROLYN ROBERTS, MORRISVILLE, VT, ON BEHALF OF AMERICAN HOSPITAL ASSOCIATION; AND KATHLEEN A. FRAWLEY, AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION, WASHINGTON, DC

Dr. DETMER. Thank you, and good morning, Madam Chairman.

In addition to the roles that you mentioned, I also have a seat on the boards of the Association for Health Services Research, the Association for Academic Health Centers, and the American Medical Informatics Association. I mention that since I am also testifying today for two of those organizations.

I will testify today from several perspectives—as a citizen, as a patient, as a surgeon, as a medical educator, as a health services researcher, and as an academic health center administrator.

Thank you for this opportunity. I am particularly appreciative of Senators Bennett and Leahy for sponsoring this legislation, and to you and your colleagues who are the cosponsors, including Senator and Dr. Frist.

This strong bipartisan support reflects the importance of this issue for all Americans. Today, the average American does not have adequate protection of his or her personal health information. Instead, we have the patchwork of largely inadequate, uncoordinated and sometimes contradictory State laws that you just heard about from Senator Bennett.

Last year, you nearly passed such legislation, but alas, the effort died with the rest of the health reform package. This year, we must succeed.

While coming technological advantages and advances will enable better encryption of patient records, we cannot rely solely on the technology. Rather, all persons exposed to sensitive personal health care records must realize that they not only have a responsibility to protect patient confidentiality, but that sanctions exist if they ignore or abuse this responsibility. Further, those with no right or need to access such records should be put on notice.

At the same time, if we are to have a quality, cost-effective health care system, patient information must be available for direct patient care, a number of legitimate administrative purposes, as well as for health services research and critical public health efforts.

S. 1360 can achieve these objectives for the Nation while still allowing States to add additional protections for such records as mental health, HIV, and other conditions if they so choose to do so.

But the most central need for this legislation is to assure citizens that their information is far more secure than it is today. At its heart, accurate, secure patient data supports the doctor-patient relationship. A trusting relationship lies at the core of all effective healing encounters. Patients must trust that the information in their doctors' medical records is confidential, secure, thorough and accurate. This bill supports patients reviewing their own records for accuracy while improving security.

A number of forces have recently heightened the importance of confidential medical records. First is the growth of information

technology and computer-based patient records. The Information Age is upon us, with its information superhighway and national information infrastructure. This development is enormously important and will be more beneficial than harmful. But, as with highways for automobiles, good design and sensible laws are needed to govern the patient data roadway. When there were but two cars in America, they managed to crash into one another on Main Street.

Today, we simply have too many of these patient data-personal data crashes across the land to ignore them any longer. In addition, Americans are a mobile lot, and their data must be able to efficiently follow them as they traverse the Nation.

Our medical records have been woefully insufficient for too long. A 1991 Institute of Medicine study concluded that computer-based patient records are an essential technology for health care precisely because they do capture, store, and make available primary longitudinal patient data and link health care professionals electronically to relevant recent sources of medical knowledge at the time and site of care.

Two separate IOM studies in the past 5 years have argued for a confidentiality law for medical records. While research on the humane genome is just now beginning to help us relieve human misery, in the short term, it also allows genetic markers to identify individuals with a predisposition to a variety of diseases. S. 1360 allows computer-based records to support up-to-date care confidentially.

The next issue is public accountability. People want and deserve a greater stake in their own health care, and they need better information on which to make important personal health care decisions. Valid report cards on the performance of health plans can only emerge if they are constructed from accurate patient data.

And finally, and perhaps most importantly, there is the dramatic growth of managed health care and integrated delivery systems. Today, large organizations are providing services to populations of patients. As the amount of data stored in the information systems of these organizations grows, so too does the potential for abuse of these data. I believe this bill offers some real help against such abuse. By designating an employer who also offers health care through a managed care plan as a health information trustee, the requirements of the bill constrain that employer to use the data for the purposes for which they were collected, that is, for the care and management of their patients, and not as commercial databases.

Living in such dynamic times requires us to adjust our policies over time. To this end, the Secretary of Health and Human Services is mandated to use an advisory committee to assure a sensible evolution of standards and policies. It makes great sense for that committee to be the National Committee on Vital and Health Statistics, particularly since it is already well-established, highly respected, and thereby assures a strong public-private partnership.

The bill before you represents the reflected wisdom of a wide range of perspectives, but nothing is perfect. However, with the salutary effect of these hearings, desired refinements can be made, and the result will be even better legislation.

We need S. 1360, and we need it now. Tough, fair legislation which is sufficiently rigid to protect patient data, but flexible

enough to assure high-quality, efficient health care and legitimate research.

I believe the bill has struck a strong middle ground. Please keep in mind as concerns are raised today and in the days that follow that we have virtually no consistent national protection of patient information at this time; and further, that a broad array of public interest and professional groups support this bill.

Let there be no misunderstanding about this issue. This legislation is essential for any sensible development of policy and procedures for health data in the Information Age. I firmly believe the bill will help advance health care in this Nation, principally by improving confidentiality.

In summary, I urge your enthusiastic support of this legislation. I appreciate your comments at the beginning, and I thank you for the invitation to present my views. I would be happy to respond to any questions if you have them.

The CHAIRMAN. Thank you very much, Dr. Detmer.

[The prepared statement of Dr. Detmer may be found in the appendix.]

The CHAIRMAN. Ms. Scott?

Ms. SCOTT. Thank you, Madam Chairman and members of the committee for the opportunity to be here this morning, particularly thanking Senators Bennett and Leahy.

My name is Jeanne Scott, and I am director of government and legal affairs for CSI Technologies, an Oklahoma-based health care systems developer and health care transactions clearinghouse.

I am here today in my capacity as chairman of the Association for Electronic Health Care Transactions, AFEHCT. AFEHCT is the trade organization for the many vendors, suppliers, software developers and electronic transmission networks that are taking the concept of electronic data interchange, EDI, in health care from the drawing board to the operating room.

Our members include some of the largest American corporations—EDS, UNISYS, many of the Auerbachs, as well as small emerging companies such as my own—all working to bring EDI health care to reality. We are making the private sector investment to build this capability, the infrastructure that will be needed.

Our member companies will have processed this year nearly 400 million transactions in the health care field. These include primarily at this point claims, but other inquiries, eligibility inquiries about the status, authorizations in managed care, and the various remittance advice and reports of money moving in support of the data.

As we moved forward toward the processing and transmission of clinical and other medical data, telemedicine and outcomes in quality research, we expect that number 400 million to double, triple, and quadruple each year over the next few years. Future estimates for our industry are that we will be handling and processing literally tens of billions of transactions by the turn of the century.

Estimates of the administrative overhead, the paper and bureaucratic burden associated with health care delivery, vary from 14 to 35 percent. But even assuming that only half of the lowest estimate might be saved, that would be nearly $70 billion in 1995 health

care spending. Even more might be saved through the identification of ineffective, duplicative, and unnecessary services.

AFEHCT is here to support the development of national, consistent and workable medical record privacy standards that will help us to move forward to design the tools, the products and the services that will make the future delivery of health care services administratively and, perhaps most importantly, economically feasible.

Senators, the Bennett and Leahy legislation will give our industry a clear guideline in developing these needed tools—the standard that Senator Bennett referred to in his opening remarks.

AFEHCT supports workable systems that will optimize individual protections and assure that the advantages offered by electronic data interchange in health care will not be outweighed by the costs to individual privacy and personal freedom.

But optimization does not mean maximization. We have two important social goals at play here—protection of privacy of individually identifiable medical information and the development of needed cost-saving administrative systems for health care. The two should work together, and one should not impede the other.

AFEHCT has worked very closely with the committee staff and with the privacy community in bringing this legislation to bill form and introduction. At some point, however—and it may have been inadvertent—a critical change was made in the wording of the bill. The bright-line distinction between a health information trustee and a health information service entity—the members of AFEHCT—was blurred.

Companies such as my own, the companies that make up AFEHCT, were made subject to all of the same procedural requirements that would be imposed on health information trustees, even though we would only be acting as contractors to trustees and even though the procedural requirements would impose or could impose an impossible burden on the electronic processing of health care information.

The committee has to understand that health care EDI is not a single transaction. Each individual claim, inquiry, status report, or remittance may involve two, three, six, ten different processors. If, at each of these steps, there has to be a privity between the patient and the processor, and written notification of the transaction taking place, and authorization therefor, the system would very quickly bog down. What today takes place in seconds would take hours, days and weeks. The costs would go through the roof.

And would the public have any greater protection for their records? We think any additional protection would be marginal, and the optimization of personal privacy would not be achieved. The public would gain little if any additional protection, but at an enormous cost.

How, then, do we go about achieving our goal of optimizing personal privacy and assuring that administration simplification and cost savings can be achieved in the health care delivery?

The bright line I talked about needs to be clarified. We will work with staff on doing just this. We need to make sure that the members of the health information processors are not the ones who have to get the authorizations; this should be the responsibility of

the trustees. If an information processor takes on the role of a trustee, then it is subject to the trustee's obligations, as it should be. But serving only as an information processor, we have to make sure that those requirements are not imposed on that processor.

We should be held to privacy standards. I am the attorney for my company, and I lecture our employees every day on their obligations, because they do handle personal information. And we should be subject to sanctions if we violate that. We need to have these in place, and we support that. But the responsibility rests with the trustee and not with the processor.

We look forward to working with the committee. We thank you again for the opportunity to be here, and again, I will be available for any questions and clarifications.

Thank you.

The CHAIRMAN. Thank you, Ms. Scott.

[The prepared statement of Ms. Scott may be found in the appendix.]

The CHAIRMAN. Next is Ms. Carolyn Roberts, who is president and CEO of the Copley Hospital and Copley Hospital Systems in Morrisville, VT. I know Senator Jeffords was hoping to be here, but he may be tied up in negotiating dairy concerns in reconciliation; but whatever it is, I am sure it has Vermont in mind.

Welcome, Ms. Roberts.

Ms. ROBERTS. Thank you very much, Madam Chair, Senator Kennedy, and members of the committee.

I am very pleased to be here on behalf of the American Hospital Association and to have the opportunity to address the topic of confidentiality of individually identifiable patient information.

At the outset, I would like to State AHA's support for this legislation, and for the committee's prompt consideration of it.

This morning, I would like to make three main points in my oral statement; you have our written statement, I believe, for the record.

First, the American Hospital Association has a vision for the future of our health care system. We support a restructuring of the system to create community-based networks that integrate the delivery and financing of care, yielding more efficient and appropriate utilization of precious health care resources.

Health information infrastructure is central to this vision. Better coordination of care, the provision of seamless care to patients across time, sites, and providers, requires that information also moves smoothly throughout the system.

We are mindful that this also requires that we balance the need for such information with even greater protection of patients' rights to privacy.

Second, the American Hospital Association would like to applaud Senator Bennett and Senator Leahy—before whom I testified on this subject 2 years ago—and of course, Senator Jeffords and the many other members of this committee for taking a leadership role in introducing the bill.

The AHA also believes that protecting the right to privacy must be done in a uniform fashion. In examining the current system, several facts come to mind. One, laws are inconsistent from State to State, as pointed out by Senator Bennett earlier. At the least,

this is an administrative burden, especially for the growing number of multistate systems, networks, and health care companies. At worst, it precludes speedy transmission of crucial medical information across State lines and may even be an impediment to the effective protection of patient information.

Currently, as pointed out earlier, patients in 22 States have no right to see, copy or correct their own medical records, and some laws actually create obstacles to the legitimate flow of information. And fourth, laws do not go far enough to protect the privacy, as there is currently no penalty for breaking confidentiality.

We believe that the best way to achieve the goal of uniform protection is through a Federal law on the subject that preempts all State laws and gives everyone the right to see, copy and amend their medical records, and penalizes those who make unauthorized disclosures of such information.

Third, although AHA supports the principles outlined in this bill, we believe there are a few areas which need some modification. Two that I would mention here are, first, that while we recognize that many individuals will have access to protected health information, the requirements of the bill as currently drafted do pose an undue burden on individuals who merely transmit health care information, such as mentioned by Ms. Scott previously. Such individuals, who merely push a button to transmit health information from point A to point B, currently do not open or view protected information. In our reading of the bill, it seems that such individuals would be required to open and view protected information merely in order to comply with the requirements set forth in this bill. Clearly, that was not the intent of this bill.

And as this committee contemplates the appropriate oversight agency, AHA continues to believe that rather than HHS, an independent entity which is neither a payer, administrator or provider of health care services would be important to the establishment of public confidence.

We do not believe it is possible for HHS to reconcile the conflict of interest that occurs when it serves as both the regulated and the regulator.

In conclusion, Madam chairman, if our health care system is to provide both high-quality care and consumer peace of mind, we believe that Federal law must occupy the field and preempt the application of State law as to the collection, storage, processing and transmission of individually identifiable health care information, and that every individual have a right to see, copy and amend his or her medical records. We feel these principles are clearly outlined in this bill.

We look forward to working with this committee to achieve the passage of S. 1360, and thank you very much for the opportunity to be with you.

The CHAIRMAN. Thank you, Ms. Roberts.

[The prepared statement of Ms. Roberts may be found in the appendix.]

The CHAIRMAN. Ms. Frawley?

Ms. FRAWLEY. Thank you, Madam Chairman, Senator Kennedy, Senator Bennett. The American Health Information Management Association appreciates the opportunity to appear before this com-

mittee to present our views on the importance of S. 1360, the Medical Records Confidentiality Act of 1995. On behalf of AHIMA's 35,000 members, I am pleased to announce our strong support of this important legislation.

The American Health Information Management Association is the professional association which represents 35,000 credentialed specialists who, on a daily basis, are responsible for collecting, managing, and protecting the health information that is an increasingly important component of our Nation's health care delivery system.

AHIMA members work in hospitals and health care facilities throughout the United States and ensure that an individual's right to privacy is protected. Health information management professionals handle requests for health information from third-party payers, employers, researchers, attorneys, other health care providers, and local, State and Federal agencies. Our members ensure that information is disclosed pursuant to valid authorizations from the patient or his legal representative, or pursuant to statute, regulation or court order. This responsibility is not taken lightly and is complicated by the lack of uniform national guidelines or legislation.

For the past 67 years, AHIMA and its members have assumed the responsibility for protecting the confidentiality of health information. Our efforts have been complicated by the lack of Federal preemptive legislation. AHIMA believes that the Medical Records Confidentiality Act of 1995 is a solution to this dilemma as the bill establishes a code of fair information practices and a uniform national standard for the use and disclosure of individually identifiable health information.

Over the past several years, a consensus has emerged within Congress and among the general public regarding the need for Federal legislation to address this important issue. During the past several years, we have seen a number of very important reports which highlight the need for legislation; and certainly my written testimony does outline a number of these reports—the OTA report, "Protecting Privacy in Computerized Medical Information"; the IOM report, "Health Data in the Information Age"; the final OTA report, "Bringing Health Care Technologies Online"; and most importantly, a very significant survey from Equifax, which is a mid-decade consumer survey on the American public's perception of privacy and the use of computer-based patient records.

AHIMA is pleased that S. 1360 contains many of the provisions, based on a code of fair information practices, that were contained in our original model legislative language which we had provided to Senator Bennett's staff.

We strongly support the concept that individuals have the right to know who maintains health information and for what purposes that information is used. Many Americans have never seen their personal health records and are unaware of the information contained in their records. Section 101, Inspection and Copying of Protected Health Information, and Section 102, Correction or Amendment of Protected Health Information, will provide all Americans with the right to access their personal health information. These

provisions also provide for the rights of individuals to access their health information to amend errors if they do exist.

We note, however, some concerns about Sections 101 and 102, regarding inspection, copying and correction of information. These sections require all health information trustees and permit individuals to inspect and copy health information maintained by the trustee. These sections also require that trustees correct medical records upon request, or take certain actions of they refuse to make requested corrections. Since the medical record is the legal record of the physician or health care facility and is important to continuous treatment of the patient, we urge that a provision be added to exempt from Sections 101 and 102 those health information trustees who do not provide care to individuals.

AHIMA strongly believes that individuals have the right to know who maintains their information and for what purpose information is used. Health care information is extremely personal and sensitive information that, if improperly used or released, may cause significant harm to an individual's ability to obtain employment, education, insurance, credit, and other necessities of life.

Health information concerning an individual must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected. There must be limitations on the use and disclosure of individually identifiable health information, and we are pleased to note that this bill addresses these issues in Title II, Restrictions on Use and Disclosure.

Health information is used for a variety of legitimate purposes, including patient care, quality review, education, research, public health, and legal and financial interests. Regardless of the use or users, individuals must be assured that the information that they share with health care professionals will remain confidential.

We are also concerned that the language in S. 1360 is not clear on the distinction between internal access to health information by caregivers and external disclosure of health information. It is not appropriate to expect that authorizations or accounting for disclosure records be maintained for internal access to health information by caregivers. We would recommend that the language be amended to assure that no barriers are placed on providers who are trying to provide quality care to patients.

AHIMA strongly supports the need for mechanisms that will allow individuals to enforce their rights, and we are pleased to note that Title III, Sanctions, addresses both civil and criminal penalties for misuse or misappropriation of health information.

In conclusion, AHIMA extends its thanks to Senator Kassebaum, Senator Kennedy, and the members of the Senate Labor and Human Resources Committee for holding this extremely important hearing. We would also like to thank Senator Bennett, Senator Leahy, and the cosponsors of this legislation, many of whom are members of this committee, for identifying the need to enact this landmark confidentiality legislation. AHIMA has been honored to be asked to contribute to the development of S. 1360, and we are particularly grateful for the acknowledgement of our contributions by Senator Bennett and Senator Leahy at the press conference introducing this bill on October 24th.

AHIMA looks forward to working with this committee and the Congress to enact legislation to protect an individual's right to privacy and to ensure the confidentiality of individually identifiable health information.

Thank you for the opportunity to present our views.

[The prepared statement of Ms. Frawley may be found in the appendix.]

The CHAIRMAN. Thank you very much.

I guess the first question I would like to ask, because I am trying to understand it, was raised first by Ms. Scott, and I think I understand, Ms. Frawley and Ms. Roberts, that you would both agree that there is a problem in drawing a distinction between—what—an information processor and the health care provider and/or trustee. Am I framing it correctly?

Ms. SCOTT. I think, Senator Kassebaum, that is exactly right. There are two different entities. The trustee, generally speaking, is going to be the provider. The insurer—people who are in privity have a relationship to the patient. They have contact directly. These trustees in turn may use a variety of services to communicate back and forth as we move into EDI. This may be the telephone company, it may be a software developing company such as my own that develops editing packages that help them bring this material down, to code it, to do the kinds of things so that the information can go electronically from point A to point B. We are touching the same data, but as a processor of the information, not as—we are not interested in the data for Mrs. Jones' health care, but we do have access to it, clearly. But if we were required every time to notify Mrs. Jones that we were touching her data, and maybe give her access to the system, then that quick highway, that electronic switch that we have been trying to develop, starts to break down, and the administrative savings and the like that would come from this would quickly dissipate, and we would not gain anything.

So what we are trying to do is to draw the bright line. We need to be aware of our obligations to maintain privacy— and we will—of this data. But we cannot have these same limitations and procedural requirements imposed on the processor because it just breaks the system down. And in the bill, that bright line as I described it is not as clear as we would like it to be, and I think we can solve this problem and go forward.

The CHAIRMAN. Ms. Roberts?

Ms. ROBERTS. Senator, an analogy that was drawn for me earlier was that it is similar to the post office handling our letters. They are required to protect the confidentiality of mail, but they are not required to open it, read it, and then seal it and send it back to us. It is kind of a similar analogy to that with this information issue, I think.

The CHAIRMAN. Maybe I will let Senator Bennett respond. Do you feel that, with some minor adjustments in language, that the problem can be addressed?

Senator BENNETT. I would think so. Very clearly, these folks here, Madam Chairman, were very helpful in the drafting. We found a very compatible group, and this is just one that, for whatever reason, did not get cleaned up before it came to you, and as

I said in my opening comments, there comes a point where you have to quit and move it forward, and then afterward, you look at it and say, "Gee, I wish I had done that."

I have written a book, and my editors and coauthors finally said these projects are never completed—they are only abandoned. And we decided that we had looked at it so many times that, finally, we needed somebody else to look at it, and now this process is going forward, and I have no problem at all with the thing they are talking about.

The CHAIRMAN. Dr. Detmer?

Dr. DETMER. I think that distinction between internal and external is also sort of along that line; I think it is quite doable.

The CHAIRMAN. This brings me to what I wanted to ask you, and maybe it was internal and external that you spoke of, in that you believe that researchers should be allowed to use information if it has been properly authorized, I guess, by outside groups.

Dr. DETMER. Yes. We have had a human subjects review process for many years in medicine, for doing any project that relates mostly to protection of human subjects, but also to the informed consent aspect of it. These have subsequently been known as internal institutional review boards. And this is a somewhat new assignment for them, but it is really not off of what they have typically been doing, very functionally and very well, for many years in the public's interest. And it is something that is not a new process in any event and has not been for these organizations in legitimate research.

But you do need to have that authority and that authorization, and you also have two issues to meet in this. One, if you are going to have personal identifiable data, you need to give those data back as soon as you do not need them anymore. If you do not need those data, you will not get them. And second, the purposes of the study seem to be worth that invasion, if you will, or at least that trust, that is being given to do that project.

The CHAIRMAN. Do all of you agree that this would not be an undue problem, that these groups, as you say, that have been sort of peer review-type groups are very familiar with this area, and it is not expanding it in new ways?

Ms. Roberts?

Ms. ROBERTS. Yes, Senator, I would speak favorably to that as well. In another life, I worked at an organization that is near and dear to Senator Kennedy's life, and that is the Dana Farber Cancer Institute, and I participated in the institutional review board at that organization, as well as in an administrative function. And it is very clear that much of the wonderful work that has come out of institutions such as that relies heavily on access to patient information in order to really develop the medical protocols that will move the field forward.

I think it is terribly important, though, that the institutional review board continue to be an important part of this bill, because those groups are where the really hard and ethical discussions take place.

The CHAIRMAN. Thank you very much.

Senator Kennedy?

Senator KENNEDY. To come back to the institutional review boards, are you satisfied that there are sufficient representatives of the patients, for example, on the review boards, in your experience?

Ms. ROBERTS. I would defer to Dr. Detmer for his experience. Certainly in my experience, the organizations that have participated in the IRBs that I have been a part of have usually had a couple of ethicists on them, as well as patient advocates and clinical personnel. It is by no means controlled by the clinical or research people, but really heavy consideration is given to a broad-based, multidisciplinary approach to those reviews.

Dr. DETMER. Yes, I concur on that, and I appreciate your expertise in that area. Patient representatives are routinely on those. In fact, actually, it is a requirement if you are going for Federal grant support.

Senator KENNEDY. Well, you are obviously on both sides of this because you are a practicing physician as well as an academic researcher. And you are satisfied that this threads the needle in ways that protect both——

Dr. DETMER. It will be some imposition, but I think it is a price we have to pay to do these important things, and I think it is a matter where the circumstances have changed, and we need to change to meet those circumstances. So I do not think the burden it represents is something that a legitimate researcher is not willing to pay. But keep in mine, we are also patients, and we also have families who are patients, so it is that dimension that we also have a stake in.

Senator KENNEDY. So you think there might be levels of research that might have problems with it, but you are satisfied?

Dr. DETMER. I think it is doable, and I think it will also essentially say that if you don't need person-specific identifiable data for your research, you do not have to do that, and I think that is also not a bad suggestion to give to the research community.

Senator KENNEDY. Let me ask you, Dr. Detmer, some have pointed out that there is a difference and distinction between the criteria here and the NIH and the language which is included here in terms of definitions on research. Can you comment about the distinction and how it works practically, or if you wish, you can submit it; that's a pretty technical question, and I do not know whether you have had a chance to think about it.

Dr. DETMER. Well, I will give it more consideration as well, but my quick response is that a lot of the typical kinds of research protocols are for a new treatment or a new technology or a new device or something like that, whereas this is more of a health services research issue where you are looking at treatment that is currently already in the mainstream, if you will, and you are looking at how it plays out. That is oversimplified, but——

Senator KENNEDY. OK. Could you give us an answer for the record, and maybe I can define it more precisely.

Dr. DETMER. Yes.

[The information requested was not received at time of publication.]

Senator KENNEDY. Just generally for the panel, we are caught with the importance of accelerated information and more comprehensive information being available to the medical profession in

order that they can treat people better; and then there is also a public policy issue about what treatments work and what the costs of those treatments are. How do you look at this from that vantage point? Have you thought about it from that vantage point as to what those balances are and how we are going to protect privacy as well, and whether those different considerations are balanced in terms of how this legislation is shaped?

Dr. DETMER. In response, I actually was at a meeting of the National Research Council yesterday, at the National Academy. They have a new study which they have just undertaken which largely had a fair amount of discussion on exactly that point. I think with the growth of managed care and such, what becomes a traditional research project in the past might in fact become just part of the day-to-day working of a managed care company seeking to improve, if you will, the cost-effectiveness of its care.

This is going to be an evolving issue, and I think that is a group that is very good that is looking at this; it has excellent representation across all pieces of it, and I think it will help us in this. But I think that is why it is going to be impossible for this bill to create something that will never have to see any change in evolution. That is why I think having some process to continue to work on it is going to be important.

Senator KENNEDY. Do other members of the panel wish to comment?

Ms. FRAWLEY. Yes, I would just like to comment. One thing is that the bill does not preclude the use of aggregate health information. So that as long as we are not focusing on an individual—certainly, it does not preclude the use of information for research purposes, for outcomes analysis, for any of the issues facing us in terms of the costs of health care. As soon as you are concerned about the individual, then the bill imposes certain duties on the health information trustee.

So we feel that this is a good approach. We can still use aggregate health information to support a lot of our initiatives. There are circumstances where someone will need to know whom the individual is, and in that situation, they will have to get an authorization from the patient or it will have to be handled based on the way the bill is structured.

Senator KENNEDY. Ms. Roberts?

Ms. ROBERTS. And I would just add, Senator Kennedy, that you pointed out earlier that much of this is going on without legislation, that information is proliferating all over the place; and I think the thing that we are very pleased with about this bill is that it addresses the important issues of confidentiality and provides penalties for those that disclose inappropriately, which does not exist now. So the system is going to continue to develop, and the information is going to continue to be available, but we need some clear guidelines on how that happens.

And I guess in completing my statement, I would really urge the committee to continue to give very thoughtful consideration to these issues because as it goes forward for regulations to be developed from the legislation that comes out of this, hopefully, we would like to have clarity of the principles so that the regulations really flow with the intent of the bill.

So I am really very appreciative of the time and effort that is going into this bill.

Senator KENNEDY. Well, I think this has been an excellent panel, Madam Chairman. This is all in the cutting edge of the envelope in terms of information technology, and as much as we are generalists in a lot of different areas, this is a whole new responsibility as well as opportunity which we are going to have to address. So we need a lot of help in all policy areas, but I think especially in this one.

Thank you for very helpful testimony.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you.

Senator Jeffords?

Senator JEFFORDS. Madam Chairman, thank you for holding this excellent hearing, and I look forward to working along with you. I commend Senator Bennett and Senator Leahy for their work in this area, and Senator Kennedy for his excellent questions.

Carolyn, I am sorry I was not here to introduce you. I have read your statement. This is a busy time. We are all working very hard to make sure all those Federal employees lusting to get back to work can get there as soon as possible.

I just have a brief statement and then a question. This landmark privacy legislation, which is intended to create strong, comprehensive privacy safeguards for the health data of all Americans, the Medical Records Confidentiality Act, must facilitate medical caregivers in utilizing information technology while protecting the privacy of personal medical information.

Quality medical care involves the collection of large amounts of information by health care providers. As the delivery system in this country quickly develops into integrated networks of care, this information is no longer just between an individual and his or her doctor.

We must ensure that this information is protected so that Americans do not have to worry about confiding in their doctors. Medical records should be able to go where needed and get there quickly. When an individual is referred to a different provider or setting, much of his or her health information needs to be shared. The computer provides a cost-effective method for doing this.

Although medical care is a local process, State borders have very little to do with where people get their medical care. Medical information is currently crossing these borders, and there are no laws governing this transfer. With no current Federal guidance, the process is potentially haphazard, impeding information flow, and not safeguarding the information that does cross. We need to provide clear and uniform Federal laws to permit this transfer and protect Americans' right to privacy.

I believe this important piece of legislation will do much for us.

Carolyn, thank you again for your excellent testimony. When medical billing information is transmitted to payers or intermediaries, is the health care industry ensuring only relevant information is transmitted, and are there attempts to keep the patient's name off the records as much as possible, for example, using a code instead of a name? What is going on there.

Ms. ROBERTS. I think that the field at large is trying very hard to protect all appropriate information for patients, but I think that the absence of clear guidelines and direction on that means that perhaps it is not a consistent approach to the protection of such information, and it would be helpful to us as a field.

I would like to say that in our organization, we are very good at that, and I think that is true, and I know that all organizations, all hospitals and physician practices try very hard to protect—it is an ethic for the field to protect patient information, but it is not always possible and easy to do.

Senator JEFFORDS. Ms. Frawley, with the complexity outlined by Jeanne Schulte Scott, do you feel the record of disclosure should involve all intermediaries, processors, and value-added networks?

Ms. FRAWLEY. The important issue on the accounting for disclosure is that a patient needs to know where his or her information is and where it has flowed through the system.

Presently, if a medical record leaves a health care facility and goes to an insurer who subcontracts with different organizations, that patient has no idea who has had access to his or her health information. And as we know right now, health information may be erroneously keypunched; there may be data that is incorrect. And the patient has no way of knowing who has had access to that information.

So that AHIMA truly believes that anyone who handles, transmits or processes health information needs to maintain an accounting for disclosure, so that patient knows where the information has gone in the chain.

Now, it does not mean—the points that were brought out in Jeanne's testimony—since they do not open the envelope that contains all that information, I think there has got to be a record that they handled a transaction; but certainly for the health care professionals, there would need to be greater accountability. We would certainly have to maintain much more rigorous accounting records than many of Jeanne's organizations.

Senator JEFFORDS. Thank you.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you, Senator Jeffords.

Senator Bennett?

Senator BENNETT. I have no questions.

The CHAIRMAN. I would just like to ask Dr. Detmer one more question. You have done a lot of work on State privacy laws—as many of you have, but I know you have spent quite a bit of time reviewing such. Have you found anything in any of the current State laws that you feel was really very strong and good, that maybe has not been or could be looked at in this legislation? Is there anything you would recommend?

Dr. DETMER. I think we have laid down quite a good foundation, but I must say, with your direct question to me, I will pursue that and get back to you as well.

The CHAIRMAN. I would just like to point out that Dr. Detmer's work may be in Virginia, but his roots are in Kansas, so I always feel he has a lot of good common sense.

Thank you very much. It has been very interesting and very informative testimony, and we appreciate it.

It is a pleasure to welcome Senator Leahy now, and we would invite your comments, Senator. You have missed some of the praise that has been heaped upon you and Senator Bennett for your work in this area.

Senator Leahy has been a longtime advocate and interested in trying to find some answers to this, and Senator Bennett acknowledged working with you on this legislation that is, I think, a very important bill in addressing a complex issue that has been fraught with difficulties in finding a solution that you two have now put together in a way that seems very constructive.

Senator Leahy?

Senator BENNETT. Madam Chairman.

The CHAIRMAN. Senator Bennett, please.

Senator BENNETT. Madam Chairman, before he begins, I cannot pass up the opportunity to point out that in addition to his roots in Kansas, Dr. Detmer taught at the University of Utah.

Senator LEAHY. And we are glad to have Carolyn Roberts from Vermont here, too.

Ms. ROBERTS. Whose parents are from Kansas, I would say to the Senator. [Laughter.]

STATEMENT OF HON. PATRICK J. LEAHY, A UNITED STATES SENATOR FROM VERMONT

Senator LEAHY. Well, to quote the late Tip O'Neill, all politics is local.

Madam Chairman, I appreciate it. I was told of the kind words that were said, and I do appreciate it, as well as your having this hearing. I apologize for being late, but as I think came out, I was at the CIA, and it took much longer than I had expected.

But having you and my colleague and friend, Senator Jeffords and Senator Bennett here, I know that we are concerned about a number of these things, and I will put my whole statement in the record, but if I could just make a couple of points.

We have the most amazing technology imaginable, certainly in the lifetimes of the four of us, but I do not want that to lead to a loss of personal privacy or even the concern of a loss of personal privacy in such a way that people stop going to seek the kind of medical help that they should have, or to take advantage of some of the great technology.

I remember last year when Senator Dole remarked that a "compromise of privacy" that sends information about health and treatment to a national databank without a person's approval would be something that we could not accept. The American public care very much about their privacy. A Harris poll showed that 80 percent of the American people expressed particular concern about their computerized medical records. I think that if that poll had been taken in Vermont, I think Senator Jeffords and I would agree that it would be closer to 100 percent, just because in a small State like ours, we cherish privacy.

I began a series of hearings a couple of years ago in the Technology and Law Subcommittee of the Judiciary Committee, where we looked at such things as "smart cards," basically, little CD-ROMS which are credit card size, where you can carry all your medical records, including photographs of surgery you might have

had, your x-rays, your electrocardiograms, your family history, spouse, children, parents—all on this little card.

That is the good news. The bad news is exactly the same thing, because if anybody plugging that into a computer is able to pull it out and disseminate it, you may have things that none of us would want to be disseminated—and they could disseminate with no laws against that, just like if you could pull up off the computer anybody's records, you could just publish them.

I recall, in preparing for that, talking with the widow of Arthur Ashe, and she spoke about the anguish her family went through. Arthur Ashe, one of the great athletes and great Americans of all time, contracted the HIV virus during open heart surgery, through a blood transfusion. It was something that his family knew, his children knew, and they knew in fact that he was living with a death sentence. And they suddenly got a call from the press saying, "We have all of his medical records, and we are going to publish them. Would you like to make a comment?"

Well, now, this is man who is suffering through a tragedy with his family—it is enough to live with the grief of knowing you have a father and a husband who is living a death sentence, but now it is suddenly known to the whole public, and there is no law against that.

We heard testimony from a number of other people. I think that the unauthorized disclosure and misuse of personal medical information has affected insurance coverage, employment opportunities, credit, reputation, and a host of services for thousands of Americans. We need to set the matter right through comprehensive Federal privacy protection legislation, and I think that can be done.

We have such a patchwork of laws around this Nation, there is no way you can do it otherwise. You know, because of something that happened in one Judiciary Committee confirmation hearing, we passed a law to protect the record of videos that you rent. You may want to rent "Bambi" or another form of "Bambi"—I only know about this from my former life as a prosecutor—but we protect what you rent from a video store, and we do not protect the most intimate details of your life in your medical records.

What I worry about is not only the exposure of privacy, but those people who should have medical attention who will not then go to seek it. So I think these are the things we have to do. As we know, privacy is not a partisan issue. It should not be a political issue and will not be. It is something we can work together on. I have enjoyed working with Senator Bennett and Senator Jeffords and others on this. A number of groups have testified before you who are in here. I think we can do the best in the Senate to protect the strong privacy protection.

There are many other items I have put into my statement, but I would ask, Madam Chairman, that that be made part of the record.

Thank you.

The CHAIRMAN. Your full statement will be made a part of the record.

[The prepared statement of Senator Leahy may be found in the appendix.]

The CHAIRMAN. We very much appreciate your effort to come by. I know you had some real conflicts; yet this is a subject that has been important to you for some time.

Senator Kennedy is here for the hearing this morning as well, and as was commented, this is very much a bipartisan bill. It has the support of both the majority and the minority leaders of the Senate, as well as Senator Kennedy and myself on the committee and many of our committee members on both sides of the aisle. And it is such a pleasure to work on a positive piece of legislation that is important, that has been put together with a lot of thought and effort. Obviously, there are probably still some changes that can be made, but I think the framework is there that will be very important to addressing some troubling issues regarding medical information.

Senator Jeffords, do you have any questions for Senator Leahy?

Senator JEFFORDS. No; I would just commend him on his statement and for all the work he has done on this over the years. This is a concept which is very simple to understand and this ought to be the way it is. Getting it into law and making sure there is uniformity and yet adequate access is very difficult, and you and Senator Bennett have been extremely helpful in that regard, you and Senator Bennett, and we appreciate it.

Senator LEAHY. Thank you.

The CHAIRMAN. Senator Bennett?

Senator BENNETT. Well, Madam Chairman, as the "new kid on the block," I am delighted to have had the expertise and experience of someone who has been working on this issue for a long time available to us as we went through this process. I am grateful that Senator Leahy will allow this to be the "Bennett-Leahy" bill, and I am appreciative of his support and his expertise and his help.

Senator LEAHY. Well, I am delighted to have your support. I think the fact is that this is legislation that, if we really want it to work, has to be bipartisan. I think it has to demonstrate that this is not a partisan issue, that this is an issue of privacy. I know the people in Utah and in Kansas value their privacy just as we do in Vermont, and I think all people do.

The CHAIRMAN. Thank you very much, Senator Leahy. We appreciate it.

Senator LEAHY. Thank you, Madam Chairman.

The CHAIRMAN. It is a pleasure now to call the next panel. First, we welcome Aimee Berenson, who is the legislative counsel for the AIDS Action Council. Before coming to AIDS Action Council, Ms. Berenson was policy council for family law programs at the Women's Legal Defense Fund.

Next, Janlori Goldman is deputy director and co-founder of the Center for Democracy and Technology. Prior to her work at CDT, Ms. Goldman developed the Privacy and Technology Project of the Washington office of the American Civil Liberties Union.

Finally, Dr. Denise Nagel is a general psychiatrist and president of the Coalition for Patient Rights of New England. In addition, she is the chairman of the Medical Confidentiality Project of the National CPR.

It is a pleasure to welcome all three of you, and we will start with Ms. Berenson.

STATEMENTS OF AIMEE BERENSON, AIDS ACTION COUNCIL, WASHINGTON, DC; JANLORI GOLDMAN, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, DC; AND DR. DENISE M. NAGEL, COALITION FOR PATIENT RIGHTS OF NEW ENGLAND, LEXINGTON, MA

Ms. BERENSON. Thank you. Good morning, and I appreciate the opportunity to testify today.

For people living with HIV disease, confidentiality is not merely an academic concern. Americans living with this disease not only face a battle against the disease itself, but against the prejudice and discrimination that accompany it. People have lost their jobs, their homes, even their health care coverage, when their illness is disclosed.

Many people avoid early detection and treatment of HIV disease because they fear they will not be able to keep information confidential and thus protect themselves, their families and their friends.

Efforts to protect HIV-related health information on the State level have been hindered by the fact that health information generally is not protected. Thus, a State law may protect the fact that an individual has been tested for HIV; yet other information in that person's medical record—for example, the fact that he or she has been prescribed AZT—is not protected.

This means that even if every piece of information about one's HIV status were protected, the very fact that that information would be confidential, when information generally is not confidential, discloses that the person has a specially sensitive condition, probably HIV disease.

After struggling for over a decade to protect the confidentiality of people living with HIV disease, State by State, case by case, we have come to the conclusion that without strong Federal legislation, personal health information will never be adequately protected. That is why, even though we have concerns about particular aspects of this bill, which are laid out in my written testimony and which we believe should be addressed, we are here today to express our support for the bill for the following specific reasons.

First, S. 1360 provides a strong, uniform floor of protections. Most States do not have a comprehensive medical records confidentiality law, and the provisions of this bill are more comprehensive and stronger than just about any existing State law.

However, providing a floor as opposed to a ceiling of protections is critical. Over the course of the AIDS epidemic, enormous effort has gone into creating some State public health laws that provide enough protections to give people the confidence to come forward to be tested and treated for HIV. We must not undermine the progress, however limited it may be, that we have made in the last 12 years of this epidemic.

S. 1360 provides a strong floor of protections while protecting stronger laws, such as any State law relating to public or mental health, that prevents or restricts disclosure otherwise allowed under the bill and Federal confidentiality protections for individual alcohol and drug treatment records. These protections are critical in this bill; without them, we would not support it.

Second, S. 1360 places a legal duty to protect confidentiality on all individuals and entities handling personal health information. The flow of medical records information today is dangerously out of the control of the individual. For example, health care providers routinely disclose information to health management companies, which in turn subcontract with others to process that information for a variety of reasons, all without patient knowledge or consent.

S. 1360 creates important protections that do not currently exist. It establishes a comprehensive definition of protected health information, protecting all information about an individual's health. Second, by creating a comprehensive definition of health information trustees, the bill imposes a legal obligation to protect the confidentiality of medical records information on every, single individual and entity that handles that information.

Third, S. 1360 limits uses and disclosure of information. Under this bill, personal health information cannot be disclosed without the individual's consent except in specifically defined statutory situations. And by and large, these statutory exceptions actually serve to close what is now an unbounded, virtually unbounded, universe of cases in which your medical records can be used and disclosed without your knowledge or consent.

Moreover, the bill restricts all use and disclosure of information to the minimum amount necessary to accomplish the purpose of the disclosure. This minimization rule also provides that information obtained for one purpose cannot be used for another purpose without the consent of the individual.

One statutory exception of particular importance to people living with HIV involves public health. The bill does two important things in this regard. First, it separates legally authorized public health uses and disclosures of information from other types of uses and disclosures. This helps to ensure that HIV-related information obtained for public health purposes cannot be disclosed or used for nonpublic health purposes.

Second, by maintaining a fire wall between legally authorized public health activities and other types of activities, the bill protects the integrity and autonomy of State and local public health systems.

Third, the bill provides individuals with significant control over use and disclosure of personal health information. Under the bill, an individual's consent must be obtained prior to releasing information to anyone, even those with a legitimate need to know, in all but a few spelled-out circumstances. And this bill gives individuals the right to inspect and correct their own medical records, a right which is an essential prerequisite to informed decisionmaking about use and disclosure of information.

Many people believe these protections exist today. They do not. In 22 States in this country, you do not have a right to access your own records, even though everyone from doctors to insurance agents to billing companies may have access.

In conclusion, the enactment of a strong, comprehensive Federal medical records confidentiality law is critical to people living with HIV/AIDS and to all Americans. Congress has the power and the moral imperative to enact such legislation and to move us that

much slower to ending the intolerable epidemic of fear and discrimination that has accompanied AIDS in this country.

Thank you.

The CHAIRMAN. Thank you, Ms. Berenson.

[The prepared statement of Ms. Berenson may be found in the appendix.]

The CHAIRMAN. Ms. Goldman?

Ms. GOLDMAN. Thank you. I appreciate the opportunity to testify here today.

I want to say first that CDT very much applauds the efforts of Senators Bennett and Leahy in getting this bill introduced and having this hearing scheduled, and I appreciate your effort in this regard.

I have had the pleasure of working toward passage of legislation like this, both at the ACLU and now at the Center for Democracy and Technology. What we have learned is that there is a consensus around the need to have such legislation. For a variety of reasons, we have been unable to see it enacted. Last Congress, I think, while there was consensus that we needed this legislation, and it made its way into every major health care reform proposal introduced by both the Republicans and the Democrats, it was the failure of a health care reform bill to pass that kept this bill from passing. So I appreciate that acknowledgment and the opportunity to try to move this bill forward this Congress.

As we have heard from Senator Kennedy and a number of other people here today, information is being collected, put into computers, databased, networked—all, of course, toward laudable public health goals, health care reform goals, but without any strong privacy protection in place. The information is vulnerable whether it is in paper form or electronic form, and what we see as a true risk and a consequence of this is that people who do not trust that their health information will be protected will be deterred from participating. They will back away; they may just not participate in the health care process, or they may not participate fully, in a way that will jeopardize their health care. People should not have to give up their privacy in order to seek care.

One thing I would like to make clear at the outset that this bill that has been introduced, S. 1360, is the strongest information privacy bill yet considered by the Congress. It is stronger than what we looked at 20 years ago and than what we looked at 2 years ago. I applaud that, and I hope that it maintains that strength as it moves through the process.

Essentially what the bill does and what we support, as we have already heard, is that it gives people the right to see their own records and to make copies of them and to make corrections where necessary; it allows people to maintain control over their own information as it moves through the process, and it creates a trustee relationship that people who have authorized access to people's records are now trustees under the bill, and they have fiduciary and legal responsibilities under the bill.

As we heard earlier in some people's testimony, there are entities that are concerned about liability; they do not want to be covered by this bill or do not want to be covered to the fullest extent. I think that would be a mistake.

The way the bill is currently drafted, it says if you are an agent or a contractor or an employee of that trustee, the liability flows with you. You cannot escape liability just because you do not have a direct relationship with the individual. If you have access to the information, if you hold it, you should be held accountable under the bill as everybody else is.

Another provision in the bill which is critical is that it creates a warrant requirement for access by law enforcement, which we do not currently have. It also has very severe civil and criminal penalties for violation of the Act, and it leaves the States free in critical areas to develop laws that may be more protective than what we currently would have at the Federal level, particularly in the areas of mental health, public health, and where there is a doctor-patient privilege that has been established in that State.

One of the things we did in working on this bill is we looked at the existing State protections, and what we found was that the protections in this bill are stronger than anything you are going to find at the State level. We have done a State by State analysis and have found that this is the strongest protection. And where the States may be stronger in the areas, for instance, of mental and public health and privilege, those States are still going to be free to have stronger protections.

Yes, there are exceptions in this bill, but many people who have worked on it consider those exceptions to be critical. The public health area, where there are already State public health mandates for the collection of information, will be allowed to continue. This bill does not tell State public health departments what they can and cannot do, except that they may not redisclose for a different purpose.

The oversight section has an important provision in it which says that even if an oversight official gets access to the information, he cannot use it against the individual; he can use it for fraud investigation and fraud oversight, but in order to use it against an individual, they have to get a separate court order and a warrant. That may not be sufficient protection even with that, and I will get to that in the latter part of my testimony. And then, for emergency circumstances—there has been a pretty clear recognition that if you go into an emergency room and you are not able, for a variety of reasons, to sign authorization forms, and your life is in danger, that you should be treated. And if that involves disclosure of protected health information, that is a balance that many people are willing to live with in the bill.

Let me get to where I think the bill can be stronger—and we do think it can be strengthened. One is in the research section, which I know the second panel spent quite a bit of time on. The current bill allows for disclosure to researchers with a variety of protections, but without individual authorization. We think that individuals should be able to authorize the disclosure of protected health information for research purposes.

There is an analogous situation currently, where NIH-funded requires in Federal regulation that there is an informed consent procedure that says the researcher has got to get the consent of the individual unless they meet a waiver requirement which says it is impossible tog et the consent, or it would so badly damage the re-

search. But already NIH has been living with and has been imposing that requirement of informed consent where there is research going on. We would ask this committee to look at those provisions in the Federal Code and to adopt a similar consent provision, recognizing that there may need to be a waiver under certain circumstances.

The other area where we think the bill needs to be tightened is in the oversight section. Currently, the bill allows for oversight officials to have access to information without consent, but again only for these oversight activities.

I would suggest that we look at possibly an administrative summons or an administrative subpoena that the oversight official would have to present before getting access to the information. That at least puts some kind of accountability and oversight into the oversight process which we do not currently provide in this bill.

And my last major suggestion is that the warrant requirement currently in the bill is good. It is a probable cause requirement, and it is strong. But in looking at other privacy laws that we currently have in this country—for instance, the Cable Communications Act—the warrant requirement is stronger in those bills. The Cable Communications Act has a warrant requirement that provides for clear and convincing evidence that the information would be material to the investigation. It is a stronger and more restrictive standard than probable cause, and we strongly urge the committee to put that protection into this bill. I do not think it makes sense to have stronger protections for cable subscriber records or video rental lists than we would have for people's medical records.

My final comment. I would urge the committee to maintain the momentum that has been developed on this bill. There is a critical core of consensus. Even where we need to strengthen the bill, I think there are many people who agree on what needs to be strengthened.

One of the things that is very troubling and why I think this bill is urgently needed—there is a provision in the House-passed Budget Reconciliation Act which calls for the mandating of computerization for certain kinds of medical information; it is known as administrative simplification. When this committee considered health care reform last Congress, it refused to allow administrative simplification to move forward without strong privacy protections attached to it. Currently, that is not happening. The House bill has administrative simplification without privacy protections in it, and we do not think it should move forward without this bill or something like it attached to it.

In conclusion, there is an undisputed need for the legislation; everyone has said so today. There is a core of consensus for moving it forward. We look forward to working to strengthen and clarify the bill with you, and I would just urge that we not let another Congress go by without passing this very important privacy legislation.

Thank you.

The CHAIRMAN. Thank you very much, Ms. Goldman.

[The prepared statement of Ms. Goldman may be found in the appendix.]

The CHAIRMAN. Senator Kennedy must leave in a moment, and I think he would like to introduce Dr. Nagel.

Senator KENNEDY. I thank Senator Kassebaum. I wanted to introduce Dr. Nagel, a fellow Massachusetts resident, who is a practicing psychiatrist and president of the Coalition for Patient Rights of New England. She has thought about this issue for some time, and we are delighted to have her.

Dr. NAGEL. Thank you, Senator Kennedy.

The CHAIRMAN. Thank you. Dr. Nagel?

Dr. NAGEL. Thank you, Madam Chairman.

My name is Denise Nagel. I am a physician. I first trained at Duke University in pediatrics, and then in psychiatry at the Massachusetts General Hospital in Boston. I have been in clinical practice since finishing my residency 15 years ago.

Until my involvement in the issue of medical confidentiality, I have not been a political advocate or a lobbyist. I have received no reimbursement for the work I have done. I have no industry ties. In this testimony, I speak as the president of the Coalition for Patient Rights of New England, whose sole mission is to work to restore confidentiality to the doctor-patient relationship. I also speak as the chair of the Medical Confidentiality Project of the national CPR organization. In addition, I speak as a mother of two young children.

But more than anything, I am a doctor here to warn you, to implore you, to study the provisions of S. 1360 very carefully. I have, and I am convinced that it is not at all an act primarily concerned with the confidentiality of medical records. It is just the opposite. It will actually facilitate the transfer of medical information and data. It talks about informed consent and then authorizes the creation of databases without patient knowledge or consent.

It talks about individual rights, and then allows police broad authority to search databases directly instead of obtaining a specific record from the patient's doctor.

It talks about civil and criminal sanctions, and then preempts all common law and most existing and future State statutes.

It talks about ensuring personal privacy with respect to medical records, and then sets a ceiling rather than a floor on medical confidentiality.

We need Federal legislation that sets a minimum standard for medical record confidentiality rather than a maximum standard.

In spite of the good intentions of the sponsoring Senators—and I believe that the intentions are very good—S. 1360 has been written to advance the interests of certain segments of the computer, telecommunications, data processing and health care industries. With this bill, they would be able to careen full speed ahead to develop data networks that will give innumerable people access to our medical records legally and without our knowledge.

Advocates of S. 1360 say this is going on anyway, and that is why we need this bill. The industry itself will tell you that this bill is too strict and will break its back. We must not buy into this view that the loss of medical confidentiality is a done deal, or the industry pretense that it is against this bill.

If we think that just any legislation—or a law like this—will do, we will codify some of the most egregious breaches of ethics, morals, and the Hippocratic Oath that this country has ever seen.

The fact is, of course we need Federal legislation for the protection of medical confidentiality in the computer age; but we must use the capacity of computers to bend technology to our idea of privacy, dignity, and individual rights. If we want medical privacy in the computer age, we can have medical privacy in the computer age. Medical and security experts in this country and around the world are poised to help us achieve it.

I believe that the Senate and the American people want patient-centered legislation that guarantees their privacy. How many of us would confide in our doctor, let alone a mental health professional, if we knew that our record would be available online to so many? the situation is bad enough already.

One man told me that he was disqualified from buying life insurance because he once told his internist in passing that he was "down" and worried about a hostile takeover of his company. This man was not diagnosed with clinical depression, and he was not put on medication or even referred to a psychiatrist. But there it was, a note from his internist saying that he was depressed in his file, a red flag for all to see and use for purposes of discrimination and exclusion.

Just yesterday on the trip to Washington, a cab driver said to me, "I would like to get back into a relationship, but I don't want that thing on somebody's record."

I could talk for hours about all the examples I have heard. there is the man who was laid off because his employer knew he needed a kidney transplant; or the woman with PMS would could not purchase insurance; and the man with a history of manic depression who was not able to get a job. If you ask, I will go on.

Dr. Harold Eist, president-elect of the American Psychiatric Association, writes in his letter to Senator Kassebaum, quote: "No one, no matter how desperate they are, will come forward, reveal their disorders, and the hidden torments and suffering they have endured if they cannot be assured complete and absolute privacy. It was certainly not the intention of the framers of this bill that it would impede the expeditious delivery of humane medical services. In its present form, it will do this."

Right now in Great Britain, a medical information security policy is under consideration that is based on the principle of informed consent. It restricts electronic access to the treating clinicians only, and it requires anyone else to go to the doctor—not the database—to get the information.

We only need to look to Maryland to see the very different way our country is heading. Maryland has already passed a bill mandating the reporting of clinical data to the State, including easily identifiable information like birth date by day, month and year, and the ZIP Code of the patient.

People in-the-know expect that soon, Maryland will require doctors to report on every patient encounter, even those paid for by the patient. There is nothing in S. 1360 that would interfere with this compulsory data reporting. In fact, while the bill prevents States from writing more stringent privacy laws in most cases,

there is nothing in it that would preclude them from demanding more disclosure of medical information under the public health exception.

What will S. 1360 do? I am quite concerned that under this legislation, patients will not only be uninformed about the uses to which their medical information will be put, but will unfortunately be deliberately misled about it. Most patients will be asked for their consent to the disclosure of their medical information to their insurers and others for payment or treatment under section 202(a). The consent form under 202(a)(8) will imply that the information is solely for purposes of treatment or payment.

But then the bill permits the insurer or other trustee receiving the information to pass it on without consent—without consent—to the whole host of organizations covered in the exceptions.

Sections 204, 205, 206, 207, 208, 209, 210, 211 and 212 specify situations in which trustees, including doctors and health information services, can divulge patient-identified information without prior patient consent.

Thus, S. 1360 not only permits some types of such extremely objectionable disclosures to third parties without notification or consent, but its procedures will mislead patients in this respect. The patient not only will be unaware of this further dispersion of his or her personally-identified information, but will be cruelly tricked by the initial assurance that the disclosure will be solely for treatment and payment.

We need good medical privacy law. Good medical privacy law would limit the amount of sensitive personal information that insurers can demand. This bill does not do that.

We need to craft prohibitions on access to strictly limit insider access of the medical record to only those directly involved in the patient's care—period. This is what they are setting out to do in Great Britain, and Americans deserve no less.

Ninety percent of security breaches come from insider access. We saw this recently in Massachusetts in a rather dramatic example. A convicted child rapist was employed at one of our finest suburban hospitals. He used a password to access the records of nearly 1,000 girls and young women, one as young as 9.

We need to protect consumers and providers from losing out on services if they decline to participate in data networks. In all of these crucial ways, this bill does nothing to increase consumer choice and control.

I urge you to see this bill as a wake-up call. We need good Federal legislation in this area. S. 1360 represents the interests and needs of those who are in the business of maintaining and trading medical records electronically and those who are willing to surrender the right to privacy for some hoped-for greater good. A bill written from the patient's need for privacy and the patient and doctor's concern for confidentiality would be a very different bill indeed.

As I go back to my practice, I will meet with people with severe problems. They may feel suicidal. They may have developed a dependency on drugs or alcohol. They may be unable to cope with a family trauma. They may suffer sexual dysfunction. They all will want to be assured their meetings with me are confidential. They

will want to know if any records will be accessible by a party beyond the office. They will want to know what information their insurance companies and employers have a right to.

These are fair questions. In every other country I have researched, medical records remain in complete control of doctors and their patients. They should be that way here.

We should heed a warning from Dr. Ross Anderson in Great Britain. He consults to the British Medical Association and the Australian Privacy Commissioner. I quote him here: "America's problems have actually been helpful to us," he wrote. "British doctors are horrified when I show them U.S. press articles advising readers to be careful about disclosing sensitive information in a medical context. My own expectation is that if the Bennett bill is enacted as it stands, then your problems will get rapidly worse. With the fear of lawsuits removed, medical networks will proliferate; records will be ever more briskly traded; the incidence of abuse will soar, and the profession of medicine will become something different in America from what it is in the rest of the developed world. The U.S.A. badly needs a medical records confidentiality act," he goes on to say, "but this is not the one. I would urge you to oppose it as strongly as you can."

Hippocrates wrote: "Whatever in connection with my professional practice, I see or hear in the life of men which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."

This has been the basis of the doctor-patient relationship since 350 B.C.

Thank you very much.

The CHAIRMAN. Thank you, Dr. Nagel.

If I understood you correctly, you said that there should not be access to any party beyond the office; is that correct?

Dr. NAGEL. No; absolutely not, no. You misunderstood me. What I said is being done in Great Britain and in other countries is——

The CHAIRMAN. No; I understand that, but——

Dr. NAGEL [continuing]. They put the doctor as the one to release the information to the parties—perhaps I misunderstood your question; I'm sorry. It looks like you are shaking your head. So why don't you go ahead?

The CHAIRMAN. Well, I understood that, so you are suggesting that here, no one should have access unless it is through the doctor's office. The doctor would give the permission to give access.

Dr. NAGEL. The doctor should be the control person for access.

The CHAIRMAN. For all insurance purposes? I mean, are you, for instance, going——

Dr. NAGEL. No, that is not what I am saying, no. When patients sign their release for treatment and payment, that is very good. I think patients should sign a release for treatment and payment as is specified in section 202.

I do think that we can talk about ways of tightening up some of what is happening right now, for instance, in psychiatry, when managed care companies ask for details over the telephone of intimate details of someone's life and type it into the computer, when oftentimes they have decided in advance how they are going to restrict coverage, and they do not really need some of those details.

So I think there are things that can be done, but I am in no way suggesting that the information should not go to the insurer with the patient's authorization. What I am suggesting is that in section 202, where the patient signs for information for treatment and payment purposes, it then can go into the data networks, and patients are never asked for their permission about whether they want their information to go into the data networks for other purposes. And from the data networks that are serving in the shoes of the doctor as a health information trustee, they can then transfer the information in a patient-identified form out of these data networks, again without patient knowledge or consent.

The CHAIRMAN. Well, I really cannot imagine in this country every doctor and every doctor's office wanting to be the clearinghouse for all of this information.

Dr. NAGEL. For law enforcement and other purposes?

The CHAIRMAN. Yes. But also, this legislation is so much tighter than it is today for confidentiality, when anybody can get insurance data. I mean, under this legislation, if I am correct, you have to have the patient approve.

Dr. NAGEL. In fact, while this bill talks about the fact that there are not more stringent confidentiality laws in many States, in fact I have spoken with many lawyers who tell me that they are very successfully litigating in many States under common law, and this legislation would preempt all that law.

And I wanted to read to you just one quote from the American Bar Association, their monograph from July of 1995 on this issue. This is written by the people who are really the most prominent in health care law and dealing with this issue, and I wanted to read a quote from someone who should really know about this, and I will just tell you who she is very quickly. This is Adele Waller, who served on the Institute of Medicine's Committee on Regional Health Data Networks. She is the vice chairman of the American Academy of Health Care Attorneys Committee, and she is on the editorial board of the Managed Care Law Manual.

She states here in her article that "It is important to remember that all disclosure of patient information, whether by paper copies of records, by facsimile, or through a community health information network, must apply with applicable confidentiality laws."

She goes on to say, "In most States, this may technically require patient consent to store information on the network or for most redisclosures of patient information by the network."

So I think that in fact we have a lot stronger laws than people have been acknowledging here today.

The CHAIRMAN. Senator Bennett, you look like you would like to ask a question, but I would just like to ask Ms. Goldman and Ms. Berenson, who obviously are very concerned about confidentiality, if you feel that the questions raised by Dr. Nagel should be of concern, or are you comfortable, as I thought I heard you say in your testimony, that a patient confidentiality and privacy was protected, even with some reservations as you spoke of regarding research.

Ms. GOLDMAN. I share a lot of Dr. Nagel's concerns about what is currently happening in the world of health information in terms of networking and computerization of information. There, we part company.

My view is that we need this legislation regulate the collection of that information, to regulate those industries that are involved in the collection of that information, and to give individuals control over the information.

I see this bill as being a very strong privacy bill. It is giving individuals the ability to authorize disclosures. They authorize disclosure for payment and treatment, and Dr. Nagel certainly things that they should be able to authorize disclosure for payment purposes, but beyond that, if they withhold their authorization for any other purpose, they must still be treated, and they must still be paid.

One of the things that we deal with all the time in privacy legislation is consent models that are not meaningful, that are coercive, that require people to give consent in an involuntary manner or as a condition of receiving certain services. This bill is a step away from that and probably one of the first that we have seen in many years.

One of the things that I would be very wary of is looking to common law at the States, the court-made law, essentially, to protect people's privacy. It is absolutely inadequate. I do not want to leave people's privacy up to the whim of common law. Where a doctor-patient privilege has developed in a State, that is not being overruled essentially by this legislation. The doctor-patient privilege is still intact if the State law has developed sufficiently—as it has developed at all, it is left intact by this legislation. So where the States have developed common law on that area, and it is more protective, those laws will still stand, but in terms of creating a Federal standard so that people in every, single State around this country—not just those States that might have had good court decisions—have adequate protection.

Ms. BERENSON. If I may, I just want to say that I am coming from the perspective of patients, of people living with HIV disease and their experience with the health care system in this country, which is more than just doctor-patient confidentiality.

I would note that even to the extent that we believe it is very important to maintain doctor-patient confidentiality, we have too often found, as was referred to, that many, many breaches of confidentiality come from the doctor's office. The doctors who may themselves abide by the Hippocratic Oath do not necessarily have policies or practices within their offices that protect information.

Moreover, I would say that the only way that maintaining doctor-patient confidentiality is going to adequately protect the confidentiality of people's personal medical information is if you pay the doctor out-of-pocket—and that is not an option for a growing number of people living with HIV disease and many other conditions.

We cannot simply say to people: If you want privacy, pay for your own care, do not submit insurance claims, do not join a plan—do not do any of the things that are health care practice in America today.

That is the reality, and we have to protect people given that reality, and not say that your choice is get health care, have your confidentiality protected, or find some way to pay for your own health care or only obtain the health care that you can afford confidentially.

The CHAIRMAN. Thank you.

Senator Wellstone, do you mind if I call on Senator Bennett because I think he understand the legislation at least better than I do.

Senator BENNETT. I am not a member of the committee, so I do not want to intrude on those who are.

Senator WELLSTONE. I am outraged. [Laughter.] No. Go ahead.

The CHAIRMAN. Senator Bennett?

Senator BENNETT. Thank you, Madam Chairman.

Dr. Nagel, I would like to make a general statement. You say on page 2 of your testimony that this bill, and I am quoting, "has been written to advance the interests of certain segments of the computer, telecommunications, data processing and health care industries."

I assure you absolutely that that is not the case.

Dr. NAGEL. I was in no way suggesting that that was your intention, as I mentioned specifically.

Senator BENNETT. I will accept that you said I have good intentions. The implication in that sentence is that the wool was pulled over my eyes and that of my staff and the people who worked with us by these people. And again you say categorically the bill "has been written to advance the interests of certain segments of the computer, telecommunications, data processing and health care industries."

Dr. NAGEL. Yes, sir.

Senator BENNETT. None of those folks came to us to urge us to get involved in the first place. While we cast as wide a net as we possibly could in the drafting process to hear from patients' rights advocates, and to cross as wide a spectrum as we could—and yes, many of these people were involved in the process of looking at it—I reject the characterization that they have controlled this process and that patients' rights advocates or people just as sensitive to the needs of patients as you and the people whom you quote were not equally as involved in the drafting process and given every bit as much opportunity to be heard in their support. I want to make that very clear up front.

To the point that Ms. Goldman talked about, I can understand that some lawyers might well be upset at the idea that there is going to now be less litigation on the State level than their used to be. I will clearly say that is one of our purposes, for the very reasons that we have talked about. If you get litigation across a wide number of States dealing with this matter that produces common law results that are different from State to State, in a circumstance which I described in my opening testimony, where people are living on State lines and facing the circumstance where the law is different from one State to the other—they may live in Maryland, and their doctor is in Virginia, and the hospital to which they have been referred is in the District of Columbia—and different common law in all three circumstances, achieved by litigation, which the lawyers enjoy, produces a patchwork of differences that is intolerable.

And it is the intention of this legislation to remove that kind of circumstance. As I say, I am not surprised that some lawyers who enjoy their practice in the present circumstance are upset about

that, and I take the fact that they are upset about that as a demonstration that the legislation is moving in the right direction.

Dr. NAGEL. May I respond to that?

Senator BENNETT. Surely.

Dr. NAGEL. Thank you. One of the lawyers that I am referring to is the lawyer, A.G. Brightenstein, from the JRI Institute of Health, where she has litigated for many of the AIDS patients and works particularly for the patients—she is not in a high-priced, high-paying law firm; she is working really in a nonprofit organization and working for the very things that I think you have set out in this bill to try to protect. So that these are many of the lawyers that I have been working with.

Ms. BERENSON. If I may, Senator.

Senator BENNETT. Absolutely.

Ms. BERENSON. I will come out right here at this hearing and say that I am an attorney myself——

Senator BENNETT. As are most of the members of this committee.

Senator WELLSTONE. Let the record show I am not an attorney.

The CHAIRMAN. I am not either. [Laughter.]

Ms. BERENSON. And as an attorney who has been working in and around the AIDS epidemic since it unfortunately began, I can tell you that the reasons why attorneys may have to go to common law is because there are no protections under State law, or the protections are very inconsistent.

Additionally, I have to point out that currently, 39 States have been forced to pass some form of HIV-related confidentiality law. Why have they had to do that? They have had to do that because neither common law nor State statutes adequately protected people from breaches of confidentiality and the terrible, terrible consequences that result from that breach—the loss of jobs, the loss of homes, the loss of educational opportunities, the loss of health care.

The situation today is such that the holes are too big, and we need to patch the holes and create a framework so that lawyers and everyone else who wants to make sure that people's privacy is protected can do that. And I believe that this bill is an important step in the right direction.

The CHAIRMAN. Senator Wellstone has to leave; if he could just ask a question.

Senator BENNETT. Absolutely.

Senator WELLSTONE. Actually, I do not know that I can add much to what Ms. Berenson said. I view this effort by my colleague Senator Bennett to be one that is very important.

One thing that I am struggling with, though—and this question has been raised, and it is just something that I want to learn more about—is, just to take an example of psychiatric medical records—I happen to know something about the kind of discrimination that can take place against people just through my own family experience and the struggles of my brother. Under certain circumstances, these records could be released by parties other than physicians—that is my understanding—and if that is accurate, I guess what I would want to make sure of is that we define those circumstances in a very rigorous way and as narrowly as possible.

I think more than anything else, I view this as really an important reform effort, but I think that is the particular concern that I have, and I would like to work with you.

Senator BENNETT. We believe we have, Senator. And Dr. Nagel obviously believes that we have not.

Senator WELLSTONE. I understand that that was what Dr. Nagel was trying to say. But I would certainly like to have an opportunity—and I do apologize because I literally have to leave now—but I would like to have an opportunity to go over that with you because I know that is where you are heading and maybe be a part of it.

Senator BENNETT. We would welcome your participation.

Dr. NAGEL. May I make a short comment?

The CHAIRMAN. Sure.

Dr. NAGEL. When we have been talking about the disclosure of information with patient consent, it is really unclear to me why it would be in this bill that the information would be disclosed to the health information services without any patient knowledge or consent.

I would be happy to go over exactly how that appears in the bill if there is any question about whether it does, but when I have talked with a number of the people working on this bill, it seems that that is clearly what is written.

The CHAIRMAN. Dr. Goldman, did you wish to respond?

Ms. GOLDMAN. I would; thank you. I am also a lawyer and not a doctor, but I am actually proud of the affiliation.

The health information service section of this bill has provided some confusion, and I would like to just clarify a couple of things about it.

Health information services, which is a term in the bill but essentially talks about a certain function of certain entities or companies—they can happen within a hospital, they can be providing a health information service function, or it can be an outside company. They come under the bill, and they have to come under the bill in that trustee relationship. They are regulated because, for instance, if Georgetown Hospital decides that it wants to hire someone to do its claims processing or do outcomes analysis or do any kind of research, they can hire someone, but that entity as a health information service, as it would be considered under the bill, is considered a trustee. They are an agent or a contractor or an employee of the trustee. So any disclosure that happens has got to be listed on the authorization. The authorization has got to say to whom the information is going and for what purpose and under what circumstances.

That is what the authorization section is all about. It says that for payment and treatment, you have to sign an authorization on a separate sheet of paper so that you know who is getting your information and under what circumstances.

Now, for disclosures other than for payment and treatment, anything else—which we could call marketing, we could call any other disclosure—it is also an authorization, has to be an a separate form, in writing, on a separate day other than treatment, and if the individual withholds the authorization, he or she cannot be denied that payment and treatment.

That is where the health information service function comes in. They are under the bill as agents or contractors of the trustee.

The one other area where that function can be performed is that they get to receive information without authorization in order to turn identifiable information into nonidentifiable information, which many in the research community and public health community consider critical for doing outcomes analysis and research. And I do not want to speak for those groups, but they have seen that the obtaining of information in nonidentifiable form, using it in what they would call the "anonymized" or aggregate form, is critical. So in that circumstance, they do receive the information under the bill without authorization.

Dr. NAGEL. If I can just respond to that, as we talked about just a few days ago, it is not actually the case that the only way the health information services can receive the information is for the purpose of turning it into nonidentified information. Because of the way the definitions are written, in addition to including the health information services—to put them under all of the obligations of the doctor, which is set out I think to protect the patient, to put—let me make sure I am being clear here. Having the health information service as I have heard it laid out today in the same section as a health information trustee is for the purpose of protecting the patient. That is the reason that it was laid out that way, so that they came under all of the obligations as the physician did.

However, having it set up that way also allows the health information service to serve as an extension of the doctor in handling, in processing, in doing other things for the doctor.

Because, as Ms. Goldman clearly says, section 203 requires an authorization to be signed on a separate piece of paper, on a different day from treatment, if information is going to be released for purposes other than treatment or payment, all of those exceptions that I mentioned—204, 205, 206, 207, 208, 209, 210, 211 and 212—require no authorization to be signed. They are exceptions to the disclosure.

Ms. GOLDMAN. May I just address that for a moment? I know that Dr. Nagel goes through this list of the exceptions, and there are exceptions in the bill, but the exception that allows for disclosure to next of kin does have an opt-out provision, and it allows people to say, "I do not want you to disclose information to my next of kin." So it is not an exception to authorization.

The emergency circumstances, yes, would be an exception to authorization. Oversight is an exception to authorization, and I think we should tighten that. Public health, where the States currently mandate collection for public health reporting purposes, those laws continue to stand.

One of the things that has come up in discussions around this bill is that while this bill would require a warrant requirement for access by law enforcement, there are some people who think that people should still have to consent under that circumstance. And I just do not think that that is practical or realistic, or that our Justice Department is going to allow for that kind of—that is not necessarily an exception to authorization if you have a warrant requirement in there which requires the Government to show a very high level of either probable cause or clear and convincing evidence

that they need the information because it is material to an ongoing investigation.

Dr. NAGEL. I am certainly not suggesting getting that authorization for that.

The CHAIRMAN. Senator Jeffords?

Senator JEFFORDS. Let me follow this line, but also broaden it. The question is whether or not this should be the law for the country, or whether States should have the ability to improve what they feel, especially in the area of confidentiality.

I am concerned with what little knowledge—and a little knowledge is always a dangerous thing in computers—but also being a public servant and thinking about the Arthur Ashe case. Somebody has access to that record, then gives that information to a reporter, and the reporter, who will go to jail or be shot before he will reveal the source of his information, reveals it. What protection did Arthur Ashe have, or myself, of being able to determine who it was who obtained that information so that there could at least be an attempt to find out who it was who disclosed it? Is there a requirement in the bill that anyone who has access to it must first of all have some special password that is a changeable one, or something, so that it does not linger on? And would it not be better to allow the States to have some flexibility? I trust Vermont much more than I do the United States Government in protecting my confidentiality.

I would appreciate your comments on that.

Ms. GOLDMAN. I appreciate your question. What this bill would do is it would say that whomever it was who disclosed Arthur Ashe's medical record or Congresswoman Nydia Velazquez' medical record from a New York hospital—and there are a variety of other well-known examples of where information has been disclosed without authorization and clearly against the patient's wishes—this bill would severely punish those people within the institution who disclosed it without authorization.

Now, how the institution is going to monitor who gets access—the bill has a general rule in it that says the information can only be disclosed within the institution for a use that is compatible with and related to the purpose for which it was collected. So that someone who does not have a need to know and a need to see that information should not get it. And right now, the bill does not micromanage those institutions and tell them that they have to have passwords in place, but what it does say is that the Secretary of HHS shall develop regulations around security safeguards to make sure that information will be protected. It does not say exactly what those should say and that there should be a list of certain security safeguards, and it does leave a great deal of flexibility to the institutions and to the States, but it requires that some kind of security be developed.

Many institutions—and a number of earlier panelists can speak to this better than I—but a number of institutions currently have those kinds of procedures in place, that where information is in computerized form, that there must be pass codes, passwords, that there are hierarchies of access, that not just anyone can see the records, and that then creates an accounting—who has seen the record? Who may have disclosed it?

And I think it is those kinds of security measures that really do need to be in place, and we have an opportunity with the technology to see greater protections for the information than we currently have in paper form, where someone can open a file drawer, rifle through papers, and you do not necessarily leave a trace—maybe a fingerprint, but not a real trace of who has seen it—whereas with a computer, there is a much greater opportunity to know who has looked at a record, who has downloaded a record.

Dr. NAGEL. May I respond to that question?

Senator JEFFORDS. Yes.

Dr. NAGEL. A couple of points, one on the audit trails as a method of telling who has accessed the records. I was just presenting at the conference in New Orleans just a week ago, where I sat on a panel with a security specialist who put up a slide on how audit trails do not work; it has already been proven that they do not work as a solution to the problem of this, and there are a couple of reasons.

One, it is fairly obvious—when people are going to do something they should not be doing, they use someone else's password, like this fellow did when he went into the Newton-Wellesley records and accessed the 1,000 records of the young girls. The second is that anyone who is particularly knowledgeable about computers can bypass audit trails.

The other thing is that in the frequently-asked questions that accompanied the Bennett bill, one of the points was that many hospitals now have procedures which would comply with this bill for insider access, and in many hospitals, certainly in the Boston area, what we are finding is that anyone in the hospital with a password who is an authorized health care provider can access not just the health records of the patients whom they are giving treatment to, but they can access the health records of all the patients in the hospital. In fact, many of my friends who are practicing in hospitals in the Boston area have access to the entire medical database of all the patients from their home; they can pull it up right on their home computers.

So that what I would say is that we have a plan set out by England, who is leading the way in this area—the British Medical Association, as you may know, has said no to the National Health Service and said that if doctors go ahead and put their records online the way they were being asked to do that they could in fact lose their license for breach of confidentiality—they are coming up with some very good, really terrific proposals to use computers, to segregate records, to make it so that just the doctor and the health care providers and the payment people who need to see particular parts of the record could see that part. We have the technology now in place.

So I think this is a great age. I think we are going to be able to develop better confidentiality in this computer age than we had before, but only if we use it to our advantage here.

Ms. GOLDMAN. One of the things I neglected to make the point about is that even if it were difficult or impossible within an institution to figure out who did the disclosure—currently, as Dr. Nagel keeps saying, we have this horrible problem where information is widely available to anyone who can get access to it, people are

accessing records from their home, and this is a serious, serious issue in terms of the vulnerability of information, that it is hanging out there without the privacy protections on it—within an institution, if an institution after passage of this bill is in violation of the provision, if they have not complied with the compatible purpose section, and if someone gets access to information and they should not have access to it, even if that institution cannot identify that individual, they are liable under this bill. So the individual is protected even if we cannot point the finger and say, "This is the person who xeroxed the record, this is the person who downloaded it, this is who gave it to the reporter."

Currently, there may not be any protections for the Arthur Ashes and Nydya Velazquezes of the world, but with this bill, they would at least be able to say: "Such and such hospital, you violated this provision."

Senator BENNETT. That is correct, and Madam Chairman, if I could comment on that.

The CHAIRMAN. Yes.

Senator BENNETT. If someone is determined to get a list of 1,000 women for whatever his purposes, the chances are he is going to do it regardless of what the laws say. If someone is determined to break into a house, he is going to do it regardless of the laws against breaking and entering and against the security systems that are put in place and the big dog that is in the back yard. If you are determined enough to get in, you will get in.

The purpose of this legislation is to say to everybody who is involved in handling medical records: You must achieve a certain standard of prevention against those people who are determined.

Dr. Nagel, I cannot guarantee that this law will prevent the particular outrages that you have cited here—outrages that have occurred without this law and that will continue to occur if there is no Federal action in this area. But I believe that this Act will make it that much more difficult and will deter those people who do it casually now.

A child abuser who wants to get the names of 1,000 young women will probably still be able to do it if he is willing to run the risks and take the effort, just like the housebreaker will still be able to break into the house. But the casual practical joker, the person who would sell information to a reporter, the person who would inadvertently violate medical records for an HIV-positive person and thereby deny employment—those are the kinds of people that this law would prevent, would protect against and ultimately would produce a much higher level of confidentiality than anything we have now.

If you want me to automatically promise that no one will ever, in any circumstance, do anything improper, I am sorry, I cannot do that, and no law can.

Senator JEFFORDS. My bottom line question, if I may interrupt—I have to leave—was should not the State have the ability to ensure, or to better ensure if they so desire, confidentiality than might be provided by the regulations; and does this bill prohibit a State from strengthening or making better the methodology for confidentiality than the regulations might provide for?

Senator BENNETT. In certain areas, the State can indeed impose a higher standard, but recognizing that medical information moves across State lines now and increasingly will move across State lines in tremendous volume, one of the purpose of the bill is to establish a degree of uniformity so that people who are handling this can have assurance that they are complying with it.

Senator JEFFORDS. I understand that; I am not sure that the two are inconsistent.

Ms. BERENSON. They are not—if I may, because this has been an issue of such great importance to us. The bill specifically exempts from preemption any State law that exists or shall existing the future relating to public or mental health that prevents or restricts disclosure of protected health information otherwise allowed by the bill.

To the extent a State realizes or has realized that a particular type of disclosure or use that may be allowed under this bill is creating problems, it may act in the interest of public health or mental health to further restrict disclosure or use of that information. And that is very important.

Senator JEFFORDS. Did you say "ask" or "act"?

Ms. BERENSON. "Act."

Senator JEFFORDS. OK.

Ms. GOLDMAN. If I could also make another point which I know I made earlier, when we sat down and looked at this bill, we looked at all of the State laws, and we looked at the levels of protection that currently exist—and I know Senator Bennett had a chart up earlier about where are the States that have not done anything—but where the States have acted to protect confidentiality, we looked at this bill and compared it with existing State law. There is nothing currently at the State level that is stronger than this bill—nothing.

Dr. NAGEL. Well——

Ms. GOLDMAN. I would like to finish.

Dr. NAGEL. Sorry.

Ms. GOLDMAN. And in the area where the State may enact stronger legislation, in areas that are very sensitive, where there is fear of stigma and discrimination, as Aimee Berenson has pointed out, in the areas of public and mental health, where there is an existing doctor-patient privilege that is stronger, then the bill allows those States to enact stronger legislation. We have a State-by-State compendium which I am very happy to provide to the committee if you want to look at your particular State or just look at States overall. This bill really has taken a high ground. It is the strongest medical records privacy bill this Congress has yet considered.

Senator JEFFORDS. Thank you.

Ms. Nagel. Can I just comment on one State—Massachusetts. I spent much of the summer consulting to the Massachusetts Health Care Committee and Jay Kaufman, who is the chair of the subcommittee on privacy, has sent a very, very strong letter to Senator Kennedy because Massachusetts is right now trying to pass a very strong medical records privacy law, and there is a real fear that if this law were to pass, we could not move forward on this legislation that is in place.

Ms. GOLDMAN. It would be such a shame if the Congress decided to wait, as the Congress has waited for many years, before passing comprehensive legislation in the hope that some State somewhere would enact something stronger than the Bennett-Leahy bill.

The CHAIRMAN. Thank you very much. I think we have heard some very valuable and very interesting testimony, and we certainly appreciate the comments of all three of you on the concluding panel.

That concludes today's hearing.

[The appendix follows.]

APPENDIX

PREPARED STATEMENT OF DON E. DETMER, M.D.

Good morning, Madame Chairman. My name is Don E. Detmer. I am University Professor of Health Policy and Surgery and the Vice President and Provost for Health Sciences at the University of Virginia in Charlottesville where I also have an active vascular surgery practice. From 1989 to 1991, I chaired the Institute of Medicine committee on improving patient records. Today, I chair the Institute of Medicine (IOM) Board on Health Care Services and also have a seat on the Boards of the American Medical Informatics Association, the Association for Academic Health Centers, and the Association for Health Services Research.

Thank you for this opportunity to address this Committee on Senate Bill 1360 which proposes The Medical Record Confidentiality Act of 1995. My comments today are based on several perspectives. As a patient, as a surgeon, as a medical educator, as a health services researcher, and as an academic health center administrator, I have had ample opportunity to reflect upon the responsibility for, and the need to protect, patient privacy and confidentiality. At the same time, I am well acquainted with the crucial importance of gaining access to an individual patient's past records to save his or her life in an emergency, or to obtain a candid medical history for accurate diagnosis and treatment during the course of routine care. I have also witnessed the fundamental role aggregated patient data have played in finding new ways to cure disease. Thus, like other doctors, I believe medical records must be private, confidential, secure, thorough, and accurate. Further, I believe they must be available where and when needed to save individual lives, support the delivery of integrated care, meet personal needs of patients, and serve collective societal goods.

Many Americans might be surprised to learn that our nation does not have adequate protection of personal health information. In fact, we have a patchwork of largely inadequate, uncoordinated, and sometimes contradictory state laws. Just recently, a well-known singer was anguished by the unauthorized release of her medical record to the press. Although the hospital computer system in which the information was stored could identify the individual responsible for the release of the confidential information, the singer has little recourse against the culprit because the state in which the incident occurred has no privacy law and there is no federal protection for personal health data. Technological advances will enable encryption of patient records to help make computer-based records more secure than traditional paper records. But we should not rely solely on technology to protect these records. We must put all persons exposed to sensitive health records on notice that not only do they have the responsibility and duty to protect patient confidentiality, but also that sanctions exist if appropriate safeguards are not established or if willful misuse of personal health information occurs.

I am not surprised that Senator Frist is a strong cosponsor of this bill. As doctors, he and I both know that patients must feel safe to share the stories of their illnesses and their health experiences in a candid and forthright manner. Without such confidence, we cannot possibly do our jobs effectively. If patients withhold information from their doctor out of fear for personal privacy, we will have lost the very heart and soul of the doctor-patient encounter. Without a trusting environment, patients lose in terms of their own health status, they lose in terms of their satisfaction with the health care system, and finally they lose the value they would otherwise receive for their health care dollars.

By the time this bill and its companion in the House of Representatives completes the legislative process and emerges as law, it will achieve several important objectives. First and foremost, it will assure the privacy, confidentiality, accuracy and integrity of personal medical information. It will do this primarily by putting all those who handle patient information on notice that they have a responsibility to respect these data and that this responsibility cannot be ignored. Second, it lets the American public know that valuable, legitimate research and public health needs will continue to be met. Next, it creates a process to assure that the evolution of standards and policies attend to the objectives of the legislation over time—even as technology and the demands for patient information evolve. And finally, and possibly most important of all, citizens will know that when this bill is signed into law, their conversations with their doctor or nurse are more protected.

Bill 1360 creates a national standard for medical records and their use. The standard will allow the efficient and effective use of technology to allow lifesaving medical information to move from where it is stored to where it is needed when there is a right and need to know. This bill will create a national standard for privacy which is rigorous but at the same time allows medical information to cross state lines when appropriate authorization is given or when circumstances, such as

life-threatening illnesses, warrant it. Bill 1360 also appropriately recognizes that there are important insights which can be drawn from the proper use of patient information by serious and credible health services researchers. It allows use of information by legitimate researchers if their proposals have been reviewed and approved by groups capable of assessing their need for personally identifiable health care and their ability to manage these data responsibly.

To appreciate fully the acute need for and critical timing of this bill, it is necessary to understand the major forces that have heightened the stakes for confidentiality and privacy of medical records. First, there is the explosive growth of medical knowledge, particularly at the level of the human genome. Not only will this knowledge ultimately allow us to better treat human illness, in the short term it will allow genetic markers to identify individuals with a predisposition to a variety of diseases. Such information if made public could have serious implications for people's lives.

Moreover, the effectiveness of physicians and other health care professionals is dependent on our ability to keep up with the growth of medical knowledge. We are entering an ers when more illness is being newly understood than any time in human history. The wonderful research which is flowing from this nation's generous support for basic investigation will not achieve its full impact without the use of computer technology and the continuing contributions of medical informatics (i.e., computer and communication science as applied to health care).

Second is the growth of managed health care and integrated delivery systems. Unlike the days when health care was a cottage industry, today large organizations are providing services to populations of patients. As the amount of data stored in the information systems of these organizations grow, so too does the potential for abuse of the data. For example, unscrupulous health care providers can inappropriately use patient data to avoid enrolling patients with costly illnesses. Responsible data managers and managed care companies favor this legislation to create secure records, to allow development of audit trails, and to assure responsible national policies for the use of computer-based patient data in order to set the standards which will dramatically reduce, if not totally avoid, inappropriate use of such information. For example, by designating an employer who also offers health care through a managed care plan as a "health information trustee" the requirements of the bill constrain that employer to use the data solely for purposes for which they were collected.

The third challenge comes from the growth of information technology. Like the movement to managed care, the information age is upon us. Whether we like it or not, it is not going away. We will have an information super highway and a national information infrastructure. This development is enormously important and will be more beneficial than harmful. But as with highways for automobiles, there is a need for good design and also sensible laws governing the use of the road. When there were but two cars in America, they managed to crash on main street. Today, absence of national "right of the road" policies for the use of personal health data creates the potential for incompatible and contradictory state solutions. Not establishing a sensible national approach to this issue is like having roads which do not meet one another at state borders, or having cars drive on the right side of the road in some states and on the left side in others.

This issue is actual global in scope. During the past year I have spent a great deal of time examining our own laws and those of other nations with respect to health information. My research suggests that if the United States enacts this legislation, there is also the distinct probability that by working with other nations of the world, we may create sensible international standards for the emerging Global Information Infrastructure. In an era where 1 million people cross a national boundary each day through the network of air travel, this is not a trivial consideration.

Advances in information technology allow us to address the issues raised by a mobile, aging society. As our citizens live longer and experience chronic disease, more medical information is generated and needs to be well managed. As citizens travel or relocate, there is greater demand for transferability of medical information. A resident of Florida who visits grandchildren in New Jersey or a citizen who moves from California to Virginia to start a new job needs to have the information travel securely across state lines to assure proper integration of health care. Technology makes the transfer possible, but legislation is needed to ensure security.

This bill is also needed to accelerate improvement of medical records. Our medical records have been woefully insufficient for too long. A recent report showed that in 81 percent of cases in an outpatient clinic, physicians using current paper-based systems could not find all the patient information they desired during the patient's visit. A 1991 Institute of Medicine study concluded that computer-based patient records are an essential technology for health care precisely because they capture,

store, and make available primary, longitudinal patient data and link health care professionals electronically to sources of medical knowledge at the time and site of care. The continuing growth of medical knowledge and the need for valid clinical guidelines such as developed by the Agency for Health Care Policy and Research strongly argue for the growth and support of this essential technology for modern health care. Development of computer based patient records is hampered by the lack of adequate protection for patient records. We need S.1360 to assure that this greatest of all opportunities to improve information management in health care develops in a fully responsible way.

The final force growing in health care which necessitates this legislation is that of public accountability. People want and deserve a greater stake in their own health care and they need better information on which to make important personal health care decisions. The growth of report cards on the performance of various health care plans offers the potential to improve not only the cost but also the quality of care. Valid report cards can, however, only emerge if they are based upon reliable data drawn from patient data with individual identifiers removed.

Without policy such as outlined in S.1360, responsible data groups cannot manage such information bases to serve essential public functions. The same holds true for public health purposes and for health services research in our academic health centers. The responsible use of secondary data sets can only generate the intelligence needed to wisely inform individuals and the general public if they are built from reliable, accurate data. Public-private partnerships are desperately needed if we are to create sensible approaches to these most important issues. This legislation will allow us to sort our way through knowing that a firm foundation of confidentiality and use policies is on the books.

Over the past decade there has been a growing consensus that national action such as embodied in Senate Bill 1360 is sorely needed. The 1991 Institute of Medicine Report from the Committee on Improving the Patient Record identified lack of adequate protection of patient data as a major impediment to the development of computer-based patient records and called for national standards and legislation to remove this barrier. A second Institute of Medicine study released in 1994 urged Congress to pass legislation of this precise type. Excellent efforts along these lines were undertaken in the 103rd session of Congress in the form of Senate Bill 1757 and its companion House Bill 3600 and Senate Bill 1494 and its companion House Bill 3137, but these were not enacted.

This bill covers a very important and complex area of policy which will understandably create some consternation and debate over time. As mentioned, the bill wisely sets up a process to allow for prudent adjustments over time. The bill before you represents the reflected wisdom of a wide range of perspectives, including health professionals, hospitals, managed care, and the information industry, and public interest groups. While I believe the bill is an excellent one, judgments had to be made along the way. With the benefit of these hearings which I wholeheartedly support, refinements will come and the result will be better legislation. But let me assure you that we need S. 1360—legislation which is both tough but fair, sufficiently rigid to protect patient data but flexible enough to allow records to assure high quality, efficient patient care and legitimate research—and we need it now. Despite the concerns which some may raise, it is noteworthy that a broad array of professional and public groups support this bill and its comparable bill in the House of Representatives.

It is totally appropriate for this bill to come forward as a bipartisan piece of legislation because it clearly addresses an issue of importance to all Americans, regardless of the age, their race, their sex, their politics, their profession, even their economic status. Let there be no misunderstanding about this issue. This is a major piece of health legislation in our time—one which is crucial to public confidence in an era of human genetic research and managed care conglomerates—developments which can appear to put the physician at odds with the patient's own best interest. This legislation is essential for any sensible development of policy and procedures for health data in the Information Age. I firmly believe that this bill will help advance health care in this nation.

In summary, I urge your enthusiastic support of this legislation. With it, Americans can sleep better at night with respect to their medical records. As a health professional, I too can sleep better knowing that my patients can continue to safely share with me the story of their illnesses. We are aware that personal health information deserves protection and we are acting to set national standards to assure it. Thank you again for the invitation to present my views on this important issue. I would be happy to respond to any questions you may have.

PREPARED STATEMENT OF CAROLYN C. ROBERTS

Madame Chairman, I am Carolyn C. Roberts, president and chief executive officer of Copley Health System in Morrisville, Vermont, and immediate past chair of the Board of Trustees of the American Hospital Association (AHA). On behalf of the AHA's 5,000 hospitals, health care systems, networks and other providers of care, I am pleased to testify on S. 1360, the Medical Records Confidentiality Act of 1995. At the outset, I would like to state AHA's strong support for this legislation and for this committee's prompt consideration of it.

THE NEED TO PROMOTE THE HEALTH INFORMATION INFRASTRUCTURE

This country's health care system is undergoing rapid change. At AHA, we are working to direct the forces of change toward community-based health networks that integrate the financing and delivery of care. We believe that by bringing providers together into such local health networks, we can knit the now-fragmented system together for patients, as well as provide care more efficiently and cost-effectively.

A health information infrastructure is central to our vision of an integrated delivery system. By such an infrastructure, we mean an interconnected communication network capable of linking all participants in the U.S. health system. For better coordination of care to occur, information about patients must move smoothly across time, sites, and providers of care. Each health care facility and practitioner would connect to and become part of a larger shared information network. By increasing the accessibility of patient information, this electronic information infrastructure will help improve quality, increase efficiency, and control costs. When authorized, data from such a system could also flow to health care managers, payers, purchasers, policy makers, and researchers to monitor the performance of the health care system and make key decisions for the future. However, because this information will be traveling through a variety of providers, payers and health data repositories, including processing vendors and clearinghouses, it will become more vulnerable to unauthorized disclosures.

CURRENT PROBLEMS

As we move toward our goal, we are faced with the challenge of finding an acceptable balance between providing greater access to health care information and protecting a patient's right to privacy. For all the enthusiasm among those within the health care sector for moving toward computerized information systems, many Americans view the computerization of personal health information with suspicion, if not outright hostility. No obstacle to the development of this infrastructure looms larger than the public's understandable concerns about safeguarding the flow of personal health information.

As we begin to build a nationwide information infrastructure, we have an obligation to examine the currently inconsistent patchwork of laws and regulations that governs the exchange of patient information. Many state and federal laws create obstacles to legitimate sharing of health information that could yield better patient care, administrative savings, and more efficient patient management. For example, some states prohibit the use of computerized record systems by requiring that orders be written in ink (often referred to as "quill pen" laws) or by restricting the permissible health record storage media to the original paper or microfilm.

Moreover, payers and providers that operate in more than one state are required to comply with a multitude of different rules, which adds to administrative inefficiency. The burdensome and costly obligation of complying with individual—often inconsistent—state laws is obvious. Such costs add nothing to the quality of care and divert resources that could be better deployed.

Despite the number of state laws, most of which include some form of confidentiality protection, identifiable health care information still remains vulnerable to unauthorized disclosures. Many state laws still do not adequately address key issues, such as a patient's right to see, copy, and correct his or her own records, and the obligations of anyone who comes in contact with individually identifiable health care information—including but not limited to, payers, providers, processing vendors, storage vendors and utilization review organizations—to protect confidentiality. As a result, the current system promotes confusion over confidentiality and does an inadequate job of balancing the rights of patients against the pressing need to automate health care information.

Because many of these state laws were written in the context of the paper records of yesterday, they frequently do not offer sufficient security for today's world of electronic data interchange (EDI). The shared information networks of the future will

require explicit and uniform confidentiality requirements for handling health care data. Such protections need to be in place in order to provide appropriate incentives for providers and payers to move toward EDI while assuring confidentiality. A uniform federal law is the only mechanism that can ensure that individually identifiable health care information be maintained confidentially as it travels from place to place, including across state lines.

THE MEDICAL RECORDS CONFIDENTIALITY ACT OF 1995

AHA applauds the bipartisan effort led by Senator Robert Bennett (R-UT) which has resulted in the introduction of S.1360, the Medical Records Confidentiality Act of 1995. AHA believes that it is crucial to focus on the issue of maintaining health care information in a confidential and private manner as we begin restructuring the health care system.

AHA supports the principles set forth in this bill and recognizes the effort and thought that went into its preparation. In particular, there are three segments of the bill that AHA would like to highlight: first, federal preemption of state privacy laws; second, the right of patients to see, copy, and correct their records; and third, provision of sufficient penalties for unauthorized disclosure to create an effective deterrent to such disclosure.

- AHA believes that one of the most important components of any proposed confidentiality legislation is federal preemption, dealt with in Section 401, Relationship to Other Laws. AHA supports, without reservation, the comprehensive preemption called for in this bill. We believe that in order to reap the benefits of electronic information exchange while still protecting patient privacy and confidentiality, state law must be preempted to achieve uniformity regarding the collection, storage, processing and transmission of individually identifiable health care information. All personally identifiable health care information, regardless of where it originates or where it is transmitted should be handled pursuant to a uniform federal law. Additionally, federal law must create a system where confidentiality rights no longer vary from state to state—in other words the federal law should serve as both the "floor" and the "ceiling," such that no state could provide less protection or more protection. This bill, while allowing public health reporting exceptions, does an excellent job of providing complete federal preemption.
- The ability to access one's own medical record is available to individuals in only 28 states. Many of these state laws do not address key issues like a patient's right to copy and correct his or her own records. This bill, in sections 101 and 102, clearly provides individuals not only with the right to see and copy their medical records, but also gives them the opportunity to make any necessary corrections as well. In states where the ability to correct records exists, corrections must be requested in writing and are generally made as amendments to the medical record. AHA believes that every individual has a right to review his or her own medical record. This bill would replace the current patchwork of state laws that govern this issue.
- Perhaps the greatest defense against unauthorized disclosures is a penalty structure that deters such disclosure. AHA supports both the civil and criminal penalties described in this bill; we believe they will dramatically reduce unauthorized disclosures. The bill clearly outlines the process by which necessary and legitimate disclosures may be made. Any violation of these procedures would be reported to the appropriate authorities and the person(s) responsible for these unauthorized disclosures would be appropriately penalized.

SUGGESTED IMPROVEMENTS

Although AHA supports many of the principles outlined in this bill, there are several sections that we believe need further clarification or modification. These include:

- The Inspection and Copying of Protected Health Information; and, the Correction or Amendment of Protected Health Information sections (sections 101 and 102) as we mentioned above are critical components of this bill which need some clarification and modification. As currently drafted, these sections require all Health Information Trustees (a "trustee" is defined in S. 1360 as "a health care provider, health plan, health oversight agency, health researcher, public health authority, employer, insurer, school or university or health information service insofar as it creates, receives, obtains, maintains, uses, or transmits protected health information") to permit individuals to inspect and copy—with appropriate exceptions—their own medical records maintained by Trustees, and that

all Trustees correct medical records maintained by the Trustee, and that all Trustees correct medical records upon request or take certain actions if they refuse to make requested corrections. There may be instances, however, where a Trustee has merely transmitted the information from one party to another and never actually had access to the information itself. In other words, the Trustee was merely the conduit for the health information to travel from one point to another. Therefore, this particular type of Trustee should be exempt from this requirement. It is clearly not the intent of S. 1360 to have health information whose content that would not otherwise be viewed, to be viewed merely for the purpose of either inspecting, copying or amending a medical record. Nor do we believe it is the intent of the bill to have patients seek access to their medical records from Trustees whose sole responsibility is to transmit such information.

- This same theme is carried through to section 112(a), Accounting For Disclosure. This section states that an accounting of all by Trustees must be maintained. According to our understanding of the bill, the term "disclosure includes the simple transmission of information. Trustees who merely move information would now be required to "open" this information, view it and make an accounting of a disclosure instead of merely sending it to its next destination. Such trustees should be exempt from this section. Clearly, these organizations who merely transmit health information should be required to have appropriate security measures in place so that it is impossible to "tap" into this information as it moves across various sites. However, they should not be held to the same requirements as those Trustees who actually view individually identifiable health care information.
- Section 112(b) requires that records of such disclosures be maintained for 10 years. This may unnecessarily increase administrative costs. A shorter time period, such as seven years, or as long as the protected health information is retained, whichever is longer, may be more appropriate. As currently drafted, S. 1360 allows for a situation where records of disclosure are being maintained while the health information has already been destroyed.
- In section 203, Authorizations For Disclosure of Protected Health Information, Other Than for Treatment or Payment, there is no requirement that the authorization state the reason for disclosure. Disclosures of protected health information for other than treatment or payment purposes are equally sensitive, if not more so, and should be afforded the same protections. An example of such an authorized disclosure might be the examination of a medical record as a step in completion of a life insurance application. We therefore recommend that language similar to that provided in section 201(b)(1) be included in this section as well.
- Finally, the agency or oversight authority that will promulgate regulations and administer this Act should not be the Department of Health and Human Services (HHS). Although this may appear to be the logical choice, HHS, as a payer and administrator of health services, would also be subject to the requirements of this Act. The dual role of regulator and regulated appears to be a conflict of interest. The responsibility for implementing this Act should be assigned either to an existing or new administrative agency not otherwise responsible for administering or providing health care programs.

CONCLUSION

AHA believes it is essential that federal law completely preempt the application of state law regarding the collection, storage, processing and transmission of individually identifiable health care information as highlighted in this bill. If our new health care system—in which many health providers will either deliver care or share information across many jurisdictions—is to protect unauthorized disclosures of individually identifiable health care information and preserve its privacy and confidentiality, comprehensive federal legislation must be enacted that will ensure uniform and confidential treatment of identifiable health care information.

AHA supports complete federal preemption as outlined in this bill. The current system which includes so many different "rules" may in fact be an impediment to the effective protection of patient identifiable information. Instead of a framework in which different standards exist for different circumstances, we recommend that all individually identifiable health care information be handled uniformly. Health care information is highly sensitive and should be treated in a uniform manner, regardless of the nature of the information.

The two other areas where S. 1360 makes great strides are in patients' ability to see, copy and amend their records, and in the provision of clear and consistent penalties for unauthorized disclosure. AHA believes that every individual has a right to review his or her own medical record, and the current patchwork of state laws doesn't allow this. S. 1360 would afford all individuals such a right. In addition, both patients and health care providers will benefit from the civil and criminal penalties outlined in this bill, as those responsible for unauthorized disclosures will be appropriately penalized.

As this committee works towards refining this legislation, AHA recommends that the sections that deal with inspection, copying and correction of information and accounting for disclosure, allow those Trustees who merely transmit health care information, but never view the information that they transmit, be exempt from the requirements set forth in these respective sections. Without this change, the bill will allow those who would never otherwise view health care information, to view personally identifiable health care information for the sole purpose of complying with the requirements set forth in this bill. This would not only become an administrative burden, but may result in unauthorized disclosures which are clearly contrary to the intent of S. 1360.

Furthermore, AHA believes that it is important that individuals be informed as to the reason their health care information is being disclosed, regardless of whether or not it is for treatment or payment purposes. Therefore, we recommend that section 203, Authorization For Disclosure Other Than For Treatment Or Payment, require a specification of the reason that individually identifiable health care information is being disclosed.

Finally, as this committee contemplates the appropriate oversight agency, AHA continues to believe that an independent entity who is neither a payer, administrator, or provider of healthcare services would be important to the establishment of public confidence in a new health delivery environment. We do not believe it is possible for HHS to reconcile the conflict of interest that occurs when it serves as both the regulated and the regulator.

The American public is concerned about the development of a new health information system, where personal health information will easily travel through a variety of repositories. Simultaneously, all individually identifiable health care information needs and deserves to be protected regardless of the medium. As we move toward greater automation of health care information, the public must be assured that the benefits of computerizing this information substantially outweigh the potential risks of any unauthorized disclosures. AHA commends Senator Bennett and this committee, for their efforts in drafting and supporting the Medical Records Confidentiality Act of 1995. The steps you outline will do much to ensure the confidentiality and privacy of health care records and clinical encounters.

We appreciate the opportunity to present our views to this committee and look forward to working with you as the issues of reform and confidentiality move forward.

APPENDIX

Principles Governing the Protection of Health Records

The issue of the protection of confidentiality of patient information is not a new one; rather, the government has been active in this arena for many years.

In 1973, the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems set out the following principles to govern electronic data systems.

- Existence of personal data record keeping systems must be identified and not kept secret;
- Individuals should be able to find out what information is in their records and how it is used;
- Individuals should be able to prevent information that was obtained for one purpose from being used or made available for other purposes without their consent;
- Individuals should be able to correct or amend a record of identifiable information;
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must take precautions to prevent misuse of the data.

The Office of Technology Assessment (OTA) recently submitted a report entitled "Protecting Privacy in Computerized Medical Information". This report states that

the preaent aystem of protecting health care information offers a "patchwork of codes, state laws of varying scope, and Federal laws applicable to limited kinds of information." The OTA Report concludes by stating that "the present legal acheme does not provide consistent, comprehensive, protection for privacy in health care information, and it is inadequate to guide the health care industry with respect to obligations to protect the privacy of medical information in a computerized environment." The OTA report asserts that federal law is necessary to address issues of patient confidentiality and privacy.

In November 1991, HHS Secretary Sullivan convened a forum of national health care leaders to discuss the challenges of reducing administrative costs in the U.S. health care system. At the forum, several health care industry-led work groupa were created—including the Workgroup for Electronic Data Interchange (WEDI) and the Workgroup on Computerized Patient Records. Both of these Workgroupa submitted reports to the Secretary recommending ways the health care industry could begin reducing administrative costs associated with the delivery of and payment for health care, and recommended that national standards be established for protecting the confidentiality of individually identifiable health care information. The American Hospital Association participated in both groups and strongly supports the recommendation that Congress enact federal preemptive legislation governing the confidentiality of individually identifiable health care information.

WEDI, a public/private partnership consisting of health care leaders from all segments of the health care delivery and payment communities, believes that national legal standards for the protection of the confidentiality of personal health information should:

- Establish uniform requirements for the preservation of confidentiality and privacy rights in electronic health care claims processing and payment;
- Address the collection, storage, handling and transmission of individually identifiable health care data, including initial and subsequent disclosures, in electronic transactions by all public and private payers, providers of health care, and all other entities involved in the transactions;
- Ensure that preemption will not supersede state public health reporting lawa which address the particular health safety needs of a community;
- Delineate protocols for secure electronic storage and transmission of health care data;
- Specify fair information practices that ensure a proper balance between required disclosures, use of data, and patient privacy;
- Require publication of the existence of health care data banks;
- Encourage use of alternate dispute resolution mechanisms, where appropriate;
- Establish that compliance with the Act's requirements would serve as a defense to legal actions based on charges of improper disclosure;
- Impose penalties for violation of the Act, including civil damages, equitable remedies, and attorney's fees, where appropriate; and
- Provide enforcement by government officials and private, aggrieved parties.

WEDI reconvened in January 1993 and set up a Workgroup on Confidentiality/ Legal Issues to draft model legislation. This model legislation was included in a report delivered to Secretary Shalala in November of 1993. The requirements of this legislation are intended to apply to all entities, including public and private third-party payers and providers, that collect, store, process, or transmit such information in electronic form. The legislation would protect individually identifiable health care information, but would not affect federal and state laws that require reporting of identifiable information to public health authorities. It would also place oversight authority in an independent national privacy commission.

Prepared Statement of Kathleen A. Frawley

Madam Chairperson and Members of the Committee: My name is Kathleen A. Frawley, and I am Director of the Washington, DC Office of the American Health Information Management Association (AHIMA). AHIMA appreciates the opportunity to appear before the Senate Committee on Labor and Human Resources to present our views on the importance of S. 1360, the Medical Records Confidentiality Act of 1995. On behalf of AHIMA's 35,000 members, I am pleased to announce our strong support of this important legislation.

The American Health Information Management Association is the professional association which represents over 35,000 credentialed specialists who, on a daily basis,

manage and protect the health information that is an increasingly important component of our nation's health care delivery system.

AHIMA members work in hospitals and health care facilities throughout the United States and ensure that an individual's right to privacy is protected. Health information management professionals handle requests for health information from third party payers, employers, researchers, attorneys, other health care providers and local, state and federal agencies. Our members ensure that information is disclosed pursuant to valid authorizations from the patient or their legal representative, or pursuant to statute, regulation or court order. This responsibility is not taken lightly and is complicated by the lack of uniform national guidelines or legislation.

For the past 67 years, AHIMA and its members have assumed the responsibility for protecting the confidentiality of health information. Our efforts have been complicated by the lack of federal preemptive legislation. AHIMA believes that the "Medical Records Confidentiality Act of 1995" is a solution to this dilemma as the bill establishes a code of fair information practices and a uniform national standard for the use and disclosure of individually identifiable health information.

THE NEED FOR FEDERAL LEGISLATION

Over the past several years, a consensus has emerged within Congress and among the general public regarding the need for federal legislation to address this important issue. The Office of Technology Assessment (OTA) report, Protecting Privacy in Computerized Medical Information, found that current laws, in general, do not provide consistent, comprehensive protection of health information confidentiality. Focusing on the impact of computer technology, the report concluded that computerization reduces some concerns about privacy of health information while increasing others. The OTA report highlights the need for enactment of a comprehensive federal privacy law.

The public's concern about the confidentiality of health information was reflected in a poll conducted by Louis A. Harris and Associates for Equifax, Inc. The results of the Health Information Privacy Survey 1993 found that fifty-six percent (56%) of the survey participants indicated strong support for comprehensive federal legislation to protect the privacy of medical records as a part of health care reform.

The survey also indicated a strong agreement on what should be included in national privacy legislation. Ninety-six percent (96%) believe federal legislation should designate all personal medical information as sensitive and impose severe penalties for unauthorized disclosure. Ninety-five percent (95%) favor legislation that addresses individuals' rights to access their medical records and creates procedures for updating and correcting those records.

In 1994, the Institute of Medicine released a report, Health Data in the Information Age: Use. Disclosure and Privacy, which recommends that federal preemptive legislation be enacted to establish uniform requirements for the preservation of confidentiality and protection of privacy rights for health data about individuals.

The 1994 Equifax-Harris Consumer Privacy Survey focused on how the American public feels about having their medical records used for medical research and how safeguards would affect their opinions about such systems and uses. Among a list of 13 groups and organizations, doctors and nurses rank first in terms of the percentage of Americans who are "very" confident (43%) that this group properly handles personal and confidential information. Alter hearing a description about how medical records are used by researchers to study the causes of disease, 41% of those surveyed said that they would find it at least somewhat acceptable if their records were used for such research. If a federal law made it illegal for any medical researcher to disclose the identity or any identifiable details of a person whose health records had been used, 28% of those who were initially opposed to having their records used would change their position. This would increase the acceptance of this practice to over half of those surveyed (58%).

In the final Office of Technology Assessment (OTA) report, Bringing Health Care Online: The Role of Information Technologies, the issues of privacy and confidentiality were identified as particularly important areas in dealing with health information. The report noted that if there is little confidence that an electronic medical information system will protect them, then providers and patients will be unwilling to use it. The report recommends that Congress may wish to establish federal legislation and regulation with regard to privacy and confidentiality of medical information, as well as storage media for medical records and electronic data standards for storage and transmission of medical information.

The 1995 Equifax-Harris Mid-Decade Consumer Privacy Survey indicates that the American people say they are strongly concerned about threats to their personal privacy but believe business is doing a better job than government in handling per-

sonal information. A majority (58%) also now believes that privacy protection in the year 2000 will remain at least as strong as it is today if not improve. Americans appear more willing to take an active role in protecting their own privacy, with six out of 10 now reporting instances where they have refused to provide requested information. This is an increase from 42% since 1990.

The survey focused on the benefits of a computer-based patient record system. The majority of survey respondents see the trend towards a computer-based patient record system as either "very" beneficial (40%) or "somewhat" beneficial (45%). In terms of the personal benefits that a computer-based patient record system might provide, the greatest importance is attached to the benefit that enables key medical information to be sent to a doctor treating a person in an emergency situation away from home. 86% of survey respondents said that this would be "very" important to them. Nearly seven in ten people (69%) also said that a more effective presentation of past medical experiences, test results, and conditions would be "very" important to them. Finally, the elimination of a need to complete detailed forms as a result of the automatic printing of a patient's medical records and payment information would be "very" important to 55% of the public.

The survey also found that the ability of administrators to "identify sub-standard doctors and poorly run health facilities", to "improve the detection and reduction of fraudulent claims by patients, doctors and hospitals", and to "reduce the cost of health care by improving the identification of waste and inefficiency" would be very important to 79%, 76% and 74%, respectively, of the public. Seventy-four percent say the ability of medical researchers to "get better statistical data for studying the causes of diseases and testing new treatments" would be "very" Important to them.

The importance of benefits provided by computer-based patient records notwithstanding, most people say they are either "very" concerned (33%) or "somewhat" concerned (41%) about the potential negative effects of such a system. With detailed privacy safeguards in place, most people (80%) say they would be willing to have their medical records in a computerized system. Respondents indicated that a detailed privacy code would inform patients how their records are used; set rules of confidentiality; make it possible for patients to see their medical records; keep those records separate from all other consumer databases, and ensure the records are not used for marketing products to consumers.

Virtually, all respondents (98%) believe that a "patient should be able to obtain a copy of the medical record maintained about him or her by a doctor or health facility." In response to a similar question asked in 1978,91% of the public said that "people who want to should have the legal right to see their medical records held by their personal doctor and by a clinic or hospital."

Currently, only 28 states allow a patient to access their health information. There is little uniformity among state licensure laws and regulations regarding confidentiality of health information. It has been recognized that there is a need for more uniformity among the 50 states. In recent years, the National Conference of Commissioners on Uniform State Laws developed the Uniform Healthcare Information Act in an attempt to stimulate uniformity among states on health care information management issues. Presently, only two states, Montana and Washington, have enacted this model legislation. Vermont is presently attempting to enact comprehensive legislation. Clearly, efforts must be directed toward developing national standards on privacy and confidentiality.

HEALTH CARE AND THE INFORMATION AGE

The development of the national information infrastructure (NII) is a key component of healthcare reform. Efforts to reform this country's health care delivery system will rely heavily on administrative simplification and computerization of health information to control costs, improve quality of care and increase efficiency. The Institute of Medicine (IOM) report, The Computer-Based Patient Record: An Essential Technology for Health Care, recommended the adoption of computer-based patient records by the year 2000 and the formation of a nationwide health information network. However, as that report noted, there are states which require that medical records be written and signed. In order to facilitate the development of a national health information infrastructure, it is imperative that health information can be created, authenticated and retained in electronic form.

It is important to note that, currently, there are no federal laws outlining time frames for the retention of health information. Many states do have specific requirements. However, there is an absence of uniformity. As the healthcare industry moves from paper to computer-based patient records, retention guidelines must be re-examined to support the development of longitudinal records on a national level.

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

Because health information remains largely uncomputerized and unintegrated, patient information is often inaccessible at the time health care decisions are made. Highly trained health care professionals spend valuable time looking for records, contacting each other to obtain basic information, struggling to decipher handwritten entries or repeating tests because previous results could not be found or obtained quickly enough. National studies have estimated that health care providers spend on average approximately 40 percent of their time on paperwork. External users of health information, such as payers, researchers, governmental agencies and other must depend on a limited set of data that often is not transmitted electronically or sort through volumes of records for key information about an encounter.

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

One of the major prerequisites to the appropriate implementation of the computerbased patient record is the need for federal preemptive legislation to protect the confidentiality of health information. In order to move health care delivery systems into the 21st century, AHIMA believes that the nation cannot wait to enact federal preemptive confidentiality legislation. It is critical, and arguably, the most important aspect of any health care reform effort.

AHIMA'S POSITION

In February 1993, in order to address the need for federal legislation, AHIMA drafted model legislative language that outlined a code of fair information practices. This language was published in the OTA report as a model code and was used in the drafting of the "Medical Records Confidentiality Act of 1995."

There are a number of key provisions in AHIMA's model language which we believe must be essential elements of any legislation to govern the collection, use and disclosure of health care records. These include:

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

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

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

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

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

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

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

- Patient's right to know—The patient or the patient's representative has the right to know that health care information concerning the patient is maintained by any person and to know for what purpose the health care information is used.
- Restrictions on collection—Health care information concerning a patient must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected.
- Collection and use only for lawful purpose—Health care information must be collected and used only for a necessary and lawful purpose.
- Notification to patient—Each person maintaining health care information must prepare a formal, written statement of the fair information practices observed by such person. Each patient who provides health care information directly to a person maintaining health care information should receive a copy of the statement of a person's fair information practices and should receive a copy of the statement of a person's fair information practices and should receive an explanation of such fair information practices upon request.
- Restriction on use for other purposes—Health care information may not be used for any purpose beyond the purpose for which the health care information is collected, except as otherwise provided.
- Right to access—The patient or the patient's representative may have access to health care information concerning the patient, has the right to have a copy of such health care information made after payment of a reasonable charge, and, further, has the right to have a notation made with or in such health care information of any amendment or correction of such health care information requested by the patient or patient representative.
- Required safeguards—Any person maintaining, using or disseminating health care information shall implement reasonable safeguards for the security of the health care information and its storage, processing and transmission, whether in electronic or other form.
- Additional protections—Methods to ensure the accuracy, reliability, relevance, completeness and timeliness of the health care information should be instituted. If advisable, additional safeguards for highly sensitive health care information should be provided.

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

AHIMA is pleased that S. 1360 contains many of the provisions based on a code of fair information practices that were contained in the model language. We strongly support the concept that individuals have the right to know who maintains health information and for what purpose the information is used. Many Americans have never seen their personal health records and are unaware of the information contained in their records. Section 101, Inspection and Copying of Protected Health Information, and Section 102, Correction or Amendment of Protected Health Information, will provide all individuals with the right to access their personal health information. These provisions also provide for the right of individuals to access their health information to amend errors if they do exist.

We note, however, some concerns about sections 101 and 102 regarding inspection, copying and correction of information. These sections require all health information trustees to permit individuals to inspect and copy health information maintained by the trustee. These sections also require that trustees correct medical records upon request or take certain actions if they refuse to make requested corrections. Since the medical record is the legal record of the physician or health care facility and is important to continuous treatment of the patient, we urge that a provision be added to exempt from sections 101 and 102 those health information trustees who do not provide care to individuals.

AHIMA strongly believes that individuals have the right to know who maintains their health information and for what purpose the information is used. Health care information is extremely personal and sensitive information, that if improperly used or released, may cause significant harm to an individual's ability to obtain employment, education, insurance, credit, and other necessities. Health information concerning an individual must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected. There must be limitation on the use and disclosure of individually identifiable health information. The bill addresses these issues in Title II, Restrictions on Use and Disclosure. Health information is used for a variety of legitimate purposes, including patient care, quality review, education, research, public health, and legal and financial interests. Re-

gardless of the use or users, individuals must be assured that the information they share with healthcare professionals will remain confidential.

We are also concerned that the language in S. 1360 is not clear on the distinction between internal access to health information by caregivers and external disclosure of health information. It is not appropriate to expect that authorizations or accounting for disclosure records be maintained for internal access to health information by caregivers. We would recommend that the language be amended to ensure that no barriers are placed on providers who are trying to provide quality care to patients. AHIMA strongly supports the need for mechanisms that will allow individuals to enforce their rights. We are pleased to note that Title III, Sanctions, addresses civil and criminal sanctions.

In the 103rd Congress, AHIMA model language was also used in creating similar legislation: HR 4077, the "Fair Health Information Practices Act" and S. 2129, the "Health Care Privacy Protection Act." The legislative language from both HR 4077 and S. 2129 shared strong bipartisan support in the Senate and House. Just as an example of the support that the confidentiality effort maintained in the 103rd Congress, language from S. 2129 and HR 4077 was included in health care reform proposals offered by Senator Dole, Senator Chafee, the Senate Labor and Human Resources Committee, Congressman Michel, Congressman Gephardt, and others. The level of support in the 103rd Congressand now in the 104th Congress exemplifies the need to pass a strong, comprehensive federal confidentiality law.

SUMMARY

In conclusion, AHIMA extends its thanks to Senator Kassebaum, Senator Kennedy and the members of the Senate Labor and Human Resources Committee for holding this extremely important hearing. We would also like to thank Senator Bennett, Senator Leahy and the cosponsors of this legislation, many of whom are members of this committee, for identifying the need to enact this landmark confidentiality legislation. AHIMA is honored to have been asked to contribute to the development of S. 1360 and we are particularly grateful for the acknowledgment of our contributions by Senator Bennett and Senator Leahy at the press conference introducing this bill on October 24.

AHIMA looks forward to working with this Committee and the Congress to enact legislation to protect an individual's right to privacy and to ensure the confidentiality of individually identifiable health information. Thank you for the opportunity to present our views. We look forward to working with you as this bill moves through the Congress.

PREPARED STATEMENT OF SENATOR LEAHY

Chairman Kassebaum, Senator Kennedy and members of the Committee, I am pleased to testify before you today in favor of legislation to protect privacy of health care information and in support of the Medical Records Confidentiality Act of 1995, S.1360.

For the past several years, I have been engaged in efforts to make sure that Americans' expectations of privacy for their medical records are fulfilled. That is the purpose of this bill.

I do not want advancing technology to lead to a loss of personal privacy and do not want the fear that confidentiality is being compromised to deter people from seeking medical treatment or stifle technological or scientific development. The distinguished Republican Majority Leader put his finger on this problem last year when he remarked that a "compromise of privacy" that sends information about health and treatment to a national data bank without a person's approval would be something that none of us would accept. We should proceed without further delay to enact meaningful protection for our medical records and personal and confidential health care information.

I have long felt that health care reform will only be supported by the American people if they are assured that the personal privacy of their health care information is protected. Indeed, without confidence that one's personal privacy will be protected, many will be discouraged from seeking help from our health care system or taking advantage of the accessibility that we are working so hard to protect.

The American public cares deeply about protecting their privacy. This has been demonstrated recently in the Louis Harris polling announced only two weeks ago which indicated that almost 80 percent of the American people expressed particular concern about computerized medical records held in databases used without the individual's consent and that confidentiality of medical records is extremely important. I can assure you that if that poll had been taken in Vermont, it would have come in at 100 percent or close to it.

Two years ago, I began a series of hearings before the Technology and the Law Subcommittee of the Judiciary Committee. We explored the emerging smart card technology and opportunities being presented to deliver better and more efficient health care services, especially in rural areas. Technology can expedite care in medical emergencies and eliminate paperwork burdens. But it will only be accepted if it is used in a secure system protecting confidentiality of sensitive medical conditions and personal privacy. Fortunately, improved technology offers the promise of security and confidentiality and can allow levels of access limited to information necessary to the function of the person in the health care treatment and payment system.

In January 1994, we continued our hearings before that Judiciary Subcommittee and heard testimony from the Clinton Administration, health care providers and privacy advocates about the need to improve upon privacy protections for medical records and personal health care information.

In testimony I found among the most moving I have experienced in more than 20 years in the Senate, the Subcommittee heard first-hand from Representative Nydia Velasquez, our House colleague who had sensitive medical information leaked about her. She and her parents woke up to find disclosure of her attempted suicide smeared across the front pages of the New York tabloids. If any of us have reason to doubt how hurtful a loss of medical privacy can be, we need only talk to our House colleague.

Unfortunately, this is not the only horrific story of a loss of personal privacy. I have talked with the widow of Arthur Ashe about her family's trauma when her husband was forced to confirm publicly that he carried the AIDS virus and how the family had to live its ordeal in the glare of the media spotlight.

We have also heard testimony from Jeffrey Rothfeder who described in his book Privacy for Sale how a freelance artist was denied health coverage by a number of insurance companies because someone had erroneously written in his health records that he was HIV-positive.

The unauthorized disclosure and misuse of personal medical information have affected insurance coverage, employment opportunities, credit, reputation and a host of services for thousands of Americans. Let us not miss this opportunity to set the matter right through comprehensive Federal privacy protection legislation.

As I began focussing on privacy and security needs, I was shocked to learn how catch-as-catch-can is the patchwork of State laws protecting privacy of personally identifiable medical records. A few years ago we passed legislation protecting records of our videotape rentals, but we have yet to provide even that level of privacy protection for our personal and sensitive health care data.

The Commerce Department recently released a report on Privacy and the NII. In addition to financial and other information discussed in that report, there is nothing more personal that our health care information. We must act to apply the principles of notice and consent to this sensitive, personal information. Now is the time to accept the challenge and legislate so that the American people can have some assurance that their medical histories will not be the subject of public curiosity, commercial advantage or harmful disclosure. There can be no doubt that the increased computerization of medical information has raised the stakes in privacy protection, but my concern is not limited to electronic files.

As policy makers, we must remember that the right to privacy is one of our most cherished freedoms—it is the right to be left alone and to choose what we will reveal of ourselves and what we will keep from others. Privacy is not a partisan issue and should not be made a political issue. It is too important.

I am encouraged by the fact that the Clinton Administration clearly understands that "health security" must include assurances that personal health information will be kept private, confidential and secure from unauthorized disclosure. Early on the Administration's health care reform proposals provided that privacy and security guidelines would be required for computerized medical records. The Administrations's Privacy Working Group of its NII Task Force has been concerned with the formulation of principles to protect our privacy. In these regards, the President is to be commended.

The difficulties I had with the initial provisions of the Health Security Act, were the delay in Congress's consideration of comprehensive privacy legislation for several more years and the lack of a criminal penalty for unauthorized disclosure of someone's medical records.

Accordingly, back in May 1994, I introduce a bill to provide a comprehensive framework for protecting the privacy of our medical records from the outset rather than on a delayed basis. That bill was the Health Care Privacy Protection Act of 1994, S.2129. I was delighted to receive support from a number of diverse quarters. I want to thank you on this Committee for incorporating provisions drawn from last

year's Health Care Privacy Protection bill into those reported by the Labor and Human Resources Committee. These provisions were, likewise, incorporated in the Finance Committee bill, and in Senator Dole's bill and Senator Mitchell's bills. The Senate leadership in both parties acknowledges the fundamental importance of privacy.

Although Congress failed in its attempt to enact meaningful health care reform last Congress, we can and should proceed with privacy protection—whether or not a comprehensive health care reform package is resurrected this year. I am proud to say that the Medical Records Confidentiality Act that we joined in introducing in October, derives from the work we have been doing over the last several years. I am delighted to have contributed to this measure and look forward to our bipartisan coalition working for enactment of these important privacy protections.

Our bill establishes in law the principle that a person's health information is to be protected and to be kept confidential. It creates both criminal and civil remedies for invasions of privacy for a person's health care information and medical records and administrative remedies, such as debarment for health care providers who abuse others' privacy.

This legislation would provide patients with a comprehensive set of rights of inspection and an opportunity to add corrections to their own records, as well as information accounting for disclosures of those records.

The bill creates a set of rules and norms to govern the disclosure of personal health information and narrows the sharing of personal details within the health care system to the minimum necessary to provide care, allow for payment and to facilitate effective oversight. Special attention is paid to emergency medical situations, public health requirements and research.

We have sought to accommodate legitimate oversight concerns so that we do not create unnecessary impediments to health care fraud investigations. Effective health care oversight is essential if our health care system is to function and fulfill its intended goals. Otherwise, we risk establishing a publicly-sanctioned playground for the unscrupulous. Health care is too important a public investment to be the subject of undetected fraud or abuse.

I look forward to working with you as we continue to refine this legislation. I want to thank all of those who have been working with us on the issue of health information privacy and, in particular, wish to commend the Vermont Health Information Consortium, the Center for Democracy and Technology, the American Health Information Management Association, the American Association of Retired Persons, the AIDS Action Council, the Bazelon Center for Mental Health Law, the Legal Action Center, IBM Corporation and the Blue Cross and Blue Shield Association for their tireless efforts in working to achieve a significant consensus on this important matter. I understand that criticism has arisen from some quarters regarding this measure. I want to make clear that I will consider that criticism and review suggestions for modifications in the language as given in good faith and in a sincere effort to improve the bill and privacy protection. I hope that we can avoid shrillness and mean spiritedness on all sides, but I know that these are important matters about which many of us feel very strongly. It is never easy to legislate about privacy. I would suggest that our critics and detractors look at the bill against the backdrop of the lack of protection that now exists in so many places and in so many ways and the computerization of medical information. Indeed, the House-passed budget reconciliation bill has buried within it provisions that require the development and use of protocols "to make medical information available to be exchanged electronically." I would ask that they join with us in a constructive manner to create the best set of protections possible at the earliest possible time. With your leadership and longstanding commitment to personal privacy shared by Chairman Kassebaum and Senator Kennedy, I have every confidence that the Senate will proceed to pass strong privacy protection for medical records. With continuing help from the Administration, health care providers and privacy advocates we can enact provisions to protect the privacy of the medical records of the American people and make this part of health care security a reality for all Americans.

PREPARED STATEMENT OF JANLORI GOLDMAN

I. OVERVIEW

My name is Janlori Goldman and I am the Deputy Director of the Center for Democracy and Technology (CDT). I appreciate the opportunity to testify before you today on behalf of CDT in support of the Medical Records Confidentiality Act of 1995, (S.1360).

CDT is a non-profit, public interest organization founded by civil liberties advocates to advance public policies protecting civil liberties and democratic valuea in the development of new media. One of CDTa primary goals for the 104th Congress is the passage of federal legislation that establishes strong, enforceable privacy protection for personally identifiable health information. We believe the need for such legislation is the most critical information privacy issue facing our country today. Further, the passage of a medical records confidentiality bill should be viewed as an essential stepping stone to achieving other health care reform goals. The public will not have trust and confidence in the emerging health information infrastructure if their sensitive health data is vulnerable to abuse and misuse. We strongly support S.1360, and applaud Senators Robert Bennett and Patrick Leahy, as well as the bill's cosponsors for their strong leadership towards enacting medical confidentiality records legislation thia Congress.

At present, there is no comprehensive federal law to protect peoples' health records. However, a Louis Harris survey found that most people in this country mistakenly believe their personal health information is currently protected by law. And most people mistakenly believe they have a right to access their own medical information. In fact, only 26 states allow patients access to their own medical records and 34 states have conflicting confidentiality laws. A federal privacy policy is urgently needed to address the fact that the traditional doctor-patient relationship is being intruded upon by increasing demands for health information. CDT believes Congress must act to protect personally identifiable health information so that the reality of our laws will finally conform, to some extent, with the perception and desires of the American public.

To that end, CDT has been working with a diverse coalition of privacy and consumer advocates, health policy specialists and industry representatives, to develop a consensus on privacy policy for personally identifiable health information. This consortium of groups has operated with a keen understanding of the advances in technology today.

The societal impact of technological innovations, including those that allow medical records, data and images to be transferred easily over great distances, is felt across our country in significant ways. The development of a national information infrastructure and information superhighway are changing the ways we deal with each other. Traditional barriers of distance, time and location are disappearing as information and transactions become computerized, and few relationships in the health care field will remain unaffected by these changes. In the absence of any Congressional action on S.1360, the collection and use of personally identifiable health information will continue to occur within electronic networked environments without privacy protections.

But while this information revolution may hold great promise for enhancing our nation's health, CDT and others who support S.1360 believe that personal health information, in both paper and electronic form, must be handled within enforceable privacy rules. Even useful technologies pose potential risks, as conflicts may arise between an individual's need to keep health information confidential and the economic opportunities posed by the computerization of health records, from lowering the cost of processing insurance claims to selling personal medical records for marketing purposes.

Confidentiality must not be an afterthought in the design and use of information systems. A provision known as "administrative simplification" has been included in the House-passed budget reconciliation bill and mandates that certain personal health information be reported in standardized, electronic form. Although "administrative simplification" fosters the development of networked health information databases, the provision is silent on privacy. Without protections such as those incorporated in S.1360, CDT believes the "administrative simplification" section should not become law.

CDT strongly supports the Medical Records Confidentiality Act as the most comprehensive and strong privacy bill the Congress has yet considered in this area. Similar legislation was widely supported by both Republicans and Democrats during last Congress effort to enact health care reform. We commend Senator Bennett, Senator Leahy and this Committee for the leadership and commitment you have shown on this important legislation. Our testimony today outlines the need for this legislation, discussion of S.1360, and our recommendations for strengthening and clarifying several sections of the bill.

II. THE NEED AND DEMAND FOR FEDERAL PRIVACY PROTECTION

A. Consensus Exists

A consensus exists that federal legislation is needed to protect the privacy of personal health care records. At a conference in Washington, D.C. two years ago, cosponsored by the U.S. Office of Consumer Affairs, the American Health Information Management Association, and Equifax, nearly every panelist and member of Congress supported the need for making privacy an integral part of the health care reform effort underway at that time. In agreement were panelists from the American Medical Association, CIGNA Health Care, the U.S. Public Interest Research Group, Computer Professionals for Social Responsibility and IBM.

At the conference, Louis Harris and Associates released their Health Information Privacy Survey prepared with the assistance of Dr. Alan Westin, a privacy expert at Columbia University. The survey found that the majority of the public (56%) favored the enactment of strong comprehensive federal legislation governing the privacy of health care information. In fact, eighty-five percent (85%) said that protecting the confidentiality of medical records was absolutely essential or very important to them. Most people wanted penalties imposed for unauthorized disclosure of medical records (96%), guaranteed access to their own records (96%), and rules regulating third-party access.

A 1992 Harris survey showed that while a large majority of people recognize the benefits to society of innovative technology, nearly nine out of ten people believe computers make it easier for someone to improperly obtain confidential personal information. Twenty-five percent of the public believe they have been the victim of an improper disclosure of personal medical information.

In addition, a number of federal studies have concluded that a federal law is needed to protect peoples' medical records. In 1994, the Office of Technology Assessment (OTA) issued a report entitled Protecting Privacy in Computerized Medical Information, which addresses the effects of the computerization of medical records on people's privacy. In recommending comprehensive federal legislation, OTA found that:

> [t]he expanded use of medical records for non treatment purposes exacerbates the shortcomings of existing legal schemes to protect privacy in patient information. The law must address the increase in the flow of data outward from the medical care relationship by both addressing the question of appropriate access to data and providing redress to those who have been wronged by privacy violations. Lack of such guidelines, and failure to make them enforceable, could affect the quality and integrity of the medical record itself. (OTA Report, p. 44).

The Institute of Medicine (IOM) of the National Academy of Science released a study that focused on the risks and opportunities associated with protecting the privacy and confidentiality of personally-identifiable health data. The IOM report recommended that Congress enact legislation to preempt state laws to establish a uniform requirement for the confidentiality and protection of privacy rights for personally identifiable health data, and specify a Code of Fair Health Information Practices to ensure a proper balance between required disclosures, use of data, and patient privacy.

Most recently, Professor Larry Gostin concluded that a federal preemptive statute based on fair information practices was necessary to protect personal privacy as networked health information databases are growing. (80 Cornell Law Review 451 (1995).

All these efforts represent a tremendous pulling together of the public and private sector to achieve a critical goal—the passage of a health records confidentiality law. Nearly twenty years ago there was similar pressure to craft a medical records privacy law. In 1977, the federal Privacy Protection Study Commission issued a report recommending legislation to protect private sector records, including medical and insurance records. The Commission's recommendations sparked a Congressional effort to enact a medical records privacy bill. In 1980, due in part to pressure from the law enforcement community for unfettered access to health records, the legislative effort failed.

B. Negative Consequences

The unauthorized disclosure of personal health information can have disastrous consequences. New York Congresswoman Nydia Velazquez won her House seat only after overcoming the results of an unauthorized disclosure. Her medical records—including details of a bout with depression and suicide attempt—were faxed to a New York newspaper and television station during her campaign.

More common, and in some ways more troubling than the well publicized privacy invasions of public figures, are the consequences suffered by ordinary individuals whose privacy has been compromised by the disclosure of medical information.

In one instance, a journalist disguised himself as a doctor, obtained an actress medical record and published that she had been treated for a sexually transmitted disease. In another case, a physician at a large New York City medical school logged on to a computer system, discovered that a nurse was pregnant, and proceeded to publicize that information. Also, a Colorado medical student sold medical records to attorneys practicing malpractice law. These are just a few of the more well known stories; undoubtedly there are millions of similar breaches that occur either without the knowledge of the individuals harmed or outside the media's spotlight.

Further, errors in peoples medical records have been difficult to correct and control. For instance, Mary Rose Taylor of Springfield, Massachusetts went without health insurance for a year and a half because of a computer error at the Medical Information Bureau (MIB), a clearinghouse of medical information kept by insurance companies. MIB reported that Ms. Taylor had an abnormal urinalysis, even though she had only undergone a blood test. Ms. Taylor was forced to go to the insurance commissioner of her state to have the error corrected before she could finally receive health insurance.

Despite the public and private horror stories, many Americans trust that the information they share with their doctor is kept private. Indeed, the traditional nature of the doctor-patient relationship is intended to foster trust and to encourage full disclosure. However, once a patient's information is submitted to a third-party payor, or to any other entity, the ethical tie between doctor and patient evaporates. In fact, in a particularly telling statistic, 93% of those termed "leaders" in the Harris survey, including hospital CEOs, health insurance CEOs, physicians' nurses, and state regulators, believe that third party payors need to be governed by detailed confidentiality and privacy policies.

Within our current health care system, many people try to protect themselves against potential privacy violations. Some people routinely ask doctors to record a false diagnosis because they fear their employer may see their health records. Some people don't even tell their doctors everything about their medical condition for fear of losing control over this sensitive information. In psychiatric practices, it is common for many patients to ask doctors not to take notes during sessions for fear such notes could be leaked or even obtained legally with a subpoena. And some people try to avoid the creation of a record altogether by paying for medical services out-of-pocket, even though they are entitled to insurance coverage.

A few insurers have been candid enough to concede that their primary business relationship is with the employer/customer and not the employee/patient. These insurers may be reluctant to disclose individually-identifiable health information if requested by an employer, but they will comply if pressed. No federal law prevents disclosures by insurers to employers. Most patients, of course, believe the fiduciary relationship is between themselves and their doctors, and don't realize that a third party with no direct relationship to their medical treatment actually controls the information. It is intolerable to support a system in which an employer's payment of a portion of employees health care premiums, a normal part of most American employees compensation packages, amounts to employers controlling their employee's health records.

The problems that arise because of a lack of uniform, federal privacy protection for identifiable health information are often exacerbated by advances in technology. For example, at the state and local level today, employers, insurers, and health care providers are forming coalitions to develop automated and linked health care systems containing lifetime health histories on millions of Americans. The primary goals of these projects are cost reduction and improved quality of care.

Attempts are being made in some state coalitions to address the privacy, confidentiality and security of health data by crafting internal guidelines, regulations and contracts. In addition, in those states where the automation of health care information is seen as a key component of a state's health care reform package, state legislatures and public agencies are attempting to enact legislation that establishes a right of privacy in personally identifiable health care information. These states are also attempting to design effective enforcement penalties and oversight mechanisms to monitor the information practices of these newly created health data systems.

The outcome of this piecemeal, state by state, approach to protecting the privacy and security of health care information will be conflict among the states and a setback for the overall goal of privacy protection. Relegating the protection of health care information to the states' different guidelines, policies and laws leaves individuals subject to differing degrees of privacy depending upon where they receive their health care. In some instances, this means that individuals traveling across county

or state lines to receive necessary medical treatment may lose their ability to control how their personal medical information is used. Moreover, states and local governments with different rules governing the use of health care information may be prevented from sharing health care information contained in their systems with neighboring states that insufficiently protect privacy.

Health care records, in both paper and electronic form, deserve privacy protection. But the vulnerability of information to unauthorized use grows exponentially as the computer makes possible the instant sharing of information. As a 1992 study by the Workgroup for Electronic Data Interchange (WEDI) pointed out: "The paper medium is cumbersome and expensive . . . Ironically, it is the negative impact of the paper medium . . . that has minimized the risk of breaches of confidentiality. Although a breach could occur, if someone gave access to health records or insurance claim forms, the magnitude of the breach was limited by the sheer difficulty of unobtrusively reviewing large numbers of records or claim forms."

Nevertheless, technology itself is not the evil. Information systems can actually be designed to promote the confidentiality and security of personal information. For instance, a computerized system can sometimes be more closely guarded through technological devices than paper systems can sometimes be protected from prying eyes. The key is to recognize technology's potential to enhance privacy, not simply to focus on the risks technology poses to undermine privacy. There is widespread agreement among privacy and security experts that protections must be built in on the front-end; it is too difficult and risky to try to add them after the fact. Privacy and security must be viewed as the foundation on which health information networks are created. Only then can we achieve the potential for enhancing privacy and security.

III. THE MEDICAL RECORDS CONFIDENTIALITY ACT

CDT strongly supports the Medical Records Confidentiality Act. In particular, we support provisions in the bill that:

- Gives people the right to see, copy, and correct their own medical records;
- Limits disclosure of personal health information by requiring an individual's permission prior to disclosure of his or her health information by doctors, insurance companies, and other health information "trustees";
- Requires the development of safeguards for the use and disclosure of personal health information;
- Creates a warrant requirement for law enforcement access to peoples' health records;
- Imposes strict civil penalties and criminal sanctions for violations of the Act, and provides individuals with a private right of action against those who mishandle their personal medical information; and
- Preserves state and federal laws that may be more privacy protective in certain areas, such as public and mental health.

Without protections such as those embodied in S.1360, the rise of patchwork regulation and the widespread electronic transmission of records will produce the worst of both worlds—confusion and red tape for legitimate data users, as well as debilitating fear and mistrust for people seeking medical care.

IV. RECOMMENDATIONS

CDT believes that the Medical records Confidentiality Act represents a vast improvement on current law. Nevertheless, we urge that the bill be strengthened and clarified in a number of area, most notably by 1) requiring consent for disclosure to health researchers; 2) heightening the warrant requirement for law enforcement access; and 3) narrowing the scope of the oversight section.

A. Health Research

S.1360 currently allows researchers to receive protected health information without first obtaining an individual's authorization. We believe this is an unnecessarily broad exception and should be rewritten to incorporate a consent model.

We acknowledge that in some instances the use of records for health research may be a legitimate exception to the bill's authorization requirements. But CDT does not believe that the exceptions for research should be made broadly or routinely. Research does not usually require the release of identifiable data; anonymous non-identifiable data are often sufficient. In fact, research does not usually require the release of identifiable data without consent; it is often possible to get consent easily and prospectively.

CDT recommends that the research section be amended to require an individual's authorization prior to disclosure of personally identifiable information. We urge the committee to consider an analogous situation in which federal regulations that apply to NIH-funded biomedical research presume that consent will be obtained for use of personal medical records. Under those regulations, the nonconsensual release of records is only allowed when such records are required for the research to be effective, consent would be infeasible, and the projects significance outweighs the intrusion into privacy.

The regulations have worked well for years at institutions funded by the NIH. Since they acknowledge an individual's privacy interest while recognizing the value of research, we would urge the Committee to review them and to incorporate similar provisions in the bill.

B. Oversight

We believe that the use of records for authorized oversight functions may be a legitimate exception to the general rule of nondisclosure. However, we are concerned about the breadth of the exception currently in S.1360. As drafted, the oversight provisions of the bill have an almost undefined reach and could be over zealously extended. We recommend tightening this section by requiring oversight officials to obtain an administrative summons or subpoena for access to identifiable records.

We want to emphasize the importance of the general and specific limitations that are already in the bill. Under the general privacy rules of the bill, health oversight agencies cannot re-disclose identifiable information for other purposes not specially authorized. In addition, a health oversight agency may not use the information gathered in its oversight role for any actions against an individual other than those arising out of receipt or payment for health care or fraud.

With the inclusion of a legal process for access to identifiable information, CDT believes the bill will come closer to striking a fair balance between individual privacy and the government's legitimate needs to conduct audits and control fraud.

C. Law Enforcement

CDT strongly supports the creation of warrant requirement for law enforcement access to personal health records currently in S.1360. However, we urge that the proposed probable cause standard be heightened to equal the standard now in place for access to cable subscriber records. Under the Cable Communications Act of 1984, a warrant can not be issued for access to subscriber records until law enforcement can show "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and the information sought would be material evidence in the case." We believe that federal privacy protection for peoples' medical records should be at least as strong—if not stronger—than we apply to peoples' cable records.

V. CONCLUSION

CDT believes the protection of personally identifiable health information is critical to ensuring public trust and confidence in the emerging health information infrastructure. Health care reform cannot move forward without assuring the American public that the highly sensitive personal information contained in their medical records will be protected from abuse and misuse. As the Harris surveys indicate, people are highly suspicious of large scale computerization and believe that their health records are in dire need of privacy protection. If people are expected to embrace and participate in a reforming health environment, the price of their participation must not be the loss of control of sensitive personal information.

In the end, any system that fails to win the public's trust will fail to win the public's support, and we risk having individuals withdraw from full and honest participation in their own health care. To allow people to fall through the cracks because their privacy is not fully protected is too serious a matter to continue to go unaddressed by the Congress. We urge you to continue your commitment to moving forward with this critical legislation.

We have come a great distance in achieving broad consensus on the principles of health information privacy and we look forward to working with you to refine and enact S.1360.

PREPARED STATEMENT OF BARBARA SOUDER

Madam Chairperson and Members of the Committee: I am Barbara Souder, Executive Director of the Workgroup for Electronic Data Interchange, or WEDI. I am pleased to present WEDI's views on S. 1360, the Medical Records Confidentiality Act of 1995.

This testimony will: provide an overview of WEDI's efforts to date; outline WED's principles for privacy protection legislation; and comment on S. 1360, noting WEDI's concerns and suggestions for improving certain provisions of the bill.

OVERVIEW OF WEDI'S EFFORTS

WEDI was established in November 1991 to reduce administrative costs in the nation's healthcare system. WEDI, which began as a voluntary, public-private task force developed an action plan to streamline healthcare administration by standardizing electronic communications acrosa the industry.

Earlier this year, WEDI formalized its organization by incorporating as a not-for-profit corporation. It represents a broad array of interests in healthcare, including in its membership representatives of providers, payers, EDI vendors, government & consumers—all of the principal participants in healthcare today.

In July 1992, WEDI published a report to the HHS Secretary on the steps necessary to make electronic data interchange routine for the healthcare industry by 1996. The 1992 recommendations dealt with such issues as the need for standard formata for four core financial transactions, phased implementation by industry of those core transactions, the creation of incentives by public and private payers and the Congresa for increased use of EDI, the use of standardized billing content for claim submissions, the need for a unique identifier system that covers all participants in the healthcare system, and various other technical issues.

In addition, the 1992 WEDI report recommended that Congress enact federal preemptive legislation to facilitate and assure the uniform, confidential treatment of identifiable information in electronic environments.

Drawing from the work done by its Confidentiality and Legal Issues Technical Advisory Group (TAG), WEDI developed the recommendation to facilitate the achievement of its overall objective of moving to an EDI environment for healthcare transactions by 1996. To accomplish that goal, WEDI believed it necessary to remove statutory impediments such as "quill-pen" and other laws that inhibit or prevent the use of EDI for healthcare transactions. Several proposals were discuased, including the development of a model state law for adoption by all states within three years. But WEDI considered it most unlikely that all states would adopt uniform privacy legislation in the foreseeable future.

WEDI also considered proposing a federal law that sets standards for state legislation, but allows states to adopt more stringent standards. This, too, was rejected because of the need to establish a uniform regulatory environment. Accordingly, WEDI decided that the only logical option was to recommend the enactment of federal preemptive legislation governing confidentiality that would completely occupy the field.

WEDI reconvened in 1993 to resolve remaining implementation obstacles and work toward engaging all healthcare trading partners in standardized automation and electronic communication. The membership of WEDI's steering committee was expanded to include 26 national organizations representing payers, providers, consumers, federal and state healthcare governmental agencies, and businesses. Over 200 people representing all areas of the healthcare industry served in 11 TAGs.

In November 1993, WEDI released its second report, which contained recommendations regarding standards implementation and uniform data content, network architecture and accreditation, confidentiality and legal issues, unique identifiers, education and publicity, healthcare identification cards, short term strategies, state and federal roles, financial implications, coordination of benefits, and healthcare fraud prevention and detection.

With particular respect to the section regarding confidentiality and legal issues, the report included proposed federal legislation designed to:

- preserve confidentiality and privacy rights in individually identifiable healthcare information that is collected, stored, processed or transmitted in electronic form;
- preempt state laws that relate thereto, except public health reporting laws;
- establish a mechanism for promulgating regulations that delineate protocols for securing such information when collected, stored, processed or transmitted in electronic form and that set forth fair information practices;
- require publication of the existence of healthcare data banks;
- encourage the use of alternative dispute resolution mechanisms to resolve certain disputes under the Act; and
- establish penalties for violating the Act.

WEDI intended that the Act be construed broadly in order to protect individually identifiable healthcare information from improper and unauthorized disclosaurea in an electronic environment, while facilitating the prompt and universal implementation of electronic data interchange for legitimate and necessary healthcare transactiona.

Although complete copies of WEDI's 1992 and 1993 reports were furnished to all members of the Congress, we have attached copies of the 1993 Executive Summary and report of the Confidentiality and Legal Issues Technical Advisory Group, which includes the text of WEDI's proposed legislation, to my prepared testimony.

PRINCIPLES FOR PRIVACY PROTECTION

We are encouraged by the obvious interest shown by many members of the Congress in general, and this Committee in particular, in developing appropriate privacy protections and encouraging migration to electronic data interchange in the healthcare aystem. In evaluating legislation in this area, WEDI believes that certain principles should be recognized and that federal privacy legislation must:

- Preempt state laws, except public health reporting laws, that inhibit the use of electronic data interchange by the healthcare industry and relate to the preservation of privacy and confidentiality of identifiable healthcare information. WEDI believes that preemption is required in order to provide uniform rules of the road regarding privacy protection for all travelers on the healthcare information superhighway.
- Protect identifiable healthcare information wherever located and however obtained. WEDI believes that identifiable healthcare information obtained in nonpatient settinga, such as employment and insurance applicationa, merita similar protection against unauthorized disclosure.
- Designate an impartial entity to administer and enforce the law. WEDI is concerned that enforcement by a federal agency that is itself a healthcare provider or payer could lead to problems.
- Establish appropriate standards for privacy and confidentiality protection. To that end, the WEDI proposal aet forth five requirements for regulations that establish security standards.

  They are:

  1. Guarantee the individual'a right to know that identifiable healthcare information ia collected, atored, processed, and for what purpose it is used,

  2. Assure that the information is collected, processed, atored, and transmitted only as required for a legitimate purpose;

  3. Require that persons collecting information notify individuals of their rights under the Act;

  4. Guarantee an individual's right of access to information from the person collecting the information;

  5. Require persons collecting, processing, storing, or transmitting identifiable information to implement the standards and controls promulgated by the regulatory agency.
- Provide for rapid implementation. WEDI believes that, to realize the benefits from universal uae of electronic data interchange in the healthcare aystem aa soon aa possible, it is necessary to have in place appropriate and uniform rules for protecting the privacy of individuals.
- Be atraightforward and easily enforced. Although we recognize that no legislation is perfect, unnecessarily complicated legislation will make enforcement and implementation difficult.
- Provide appropriate civil and criminal penalties. WEDI believes that penalties for violations must be sufficient in order to foster compliance, yet not so high as to inhibit their imposition, and that the penaltiea suggested in the WEDI proposal, both civil and criminal, achieve the necessary balance.

COMMENTS ON S. 1360

WEDI is honored to have been asked to contribute to the development of S. 1360, and WEDI representativea have met on many occasions with congressional staff and others to discusa the various issues dealt with in the legislation.

The WEDI Board and membership has reviewed S. 1360 in light of the aforementioned principles and found that it comes close to atriking the appropriate balance between the right to privacy in healthcare information and the need to disclose identifiable data to appropriate entities for legitimate purposes, including payment, pro-

vision of care, medical research, protection of the public health, and law enforcement. Importantly, S. 1360 satisfies the need for uniformity in privacy protection by preempting state and federal laws, with appropriate exceptions for those laws dealing primarily with public health matters.

We note, however, some concerns and the absence of several provisions that we would like to address.

1. Inspection, Copying and Correction of information

Sections 101 and 102, dealing with inspection, copying and correction of protected health information, require all health information trustees to permit individuals to inspect and copy (with appropriate exceptions) medical records maintained by the trustee, and that all trustees correct medical records upon request, or take certain actions if they refuse to make requested corrections. These requirements may prove unnecessarily burdensome to those health information trustees who merely transmit protected health information and have no knowledge of its content. We urge that a provision be added to exempt from sections 101 and 102 those health information trustees who merely transmit protected health information.

2. Accounting for Disclosures

The requirement in section 112 (b) that records of disclosure of protected health information not related to treatment be maintained for at least ten years appears overlong, and will unnecessarily increase administrative costs. Furthermore, we note that records of disclosure could, under the provision, be destroyed even while the protected health information to which they relate are retained. Accordingly, we recommend that section 112 (b) be amended to require that records of disclosure for purposes not related to treatment be retained for at least seven years or as long as the protected health information itself is retained, whichever is longer.

3. Authorizations for Disclosure other than for Treatment or Payment

We believe it important for individuals to be informed of the reason for disclosure, especially when disclosure is for reasons other than treatment or payment. Accordingly, we suggest that section 203, governing authorizations for disclosure for reasons other than treatment or payment, be amended to require, as does section 202, a specification of the reason for disclosure.

4. Authorizations for Disclosure for Treatment or Payment

We are concerned that requiring written authorizations on separate forms for disclosure of protected health information for treatment and payment purposes will result in treatment and payment delays and unnecessarily increase administrative costs and documentation required. This unnecessary administrative cost and burden is especially evident where an entity such as an HMO, serving as both payer and provider, is required to obtain separate signatures on separate forms. We believe that where a single authorization is appropriate to disclose healthcare information for treatment and payment, that those few instances in which an insured does not want information disclosed for payment purposes can be handled on an exception basis.

5. Enforcement Authority

We suggest that it may be inappropriate to assign enforcement authority to the Secretary of Health and Human Services because that department is itself a payer and provider, and would be regulated under the Act. Accordingly, we urge that enforcement and administrative authority be assigned to an agency that is not a health information trustee under the Act.

6. Alternative Dispute Resolution

One of WEDI's recommendations calls for federal legislation to encourage the use of alternative dispute resolution (ADR) methods to resolve certain disputes. WEDI recognized that ADR can expedite the prompt resolution of disputes, often at less expense than litigation. Accordingly, we suggest that a provision be added requiring the responsible agency to promulgate regulations that promote the resolution of disputes arising under S. 1360 through ADR mechanisms.

SUMMARY

In conclusion, WEDI believes that in order to make possible the many benefits of universal electronic data interchange in healthcare transactions, the healthcare industry, including private and public payers, providers and vendors of information services, must be able to travel the information superhighway without having to consider 51 different rules of the road for privacy protection. WEDI believes that S. 1360 satisfies this key principle, and that by incorporating the suggestions out-

lined above, the bill will achieve the desired results, recognizing that privacy protection for individual records is an evolving issue requiring ongoing refinement.

WEDI looks forward to working with your committee and with the Congress to enact meaningful and appropriate legislation that facilitates the universal implementation of electronic data interchange in healthcare while protecting the privacy rights of individuals.

Thank you for your attention. We appreciate the opportunity to present our views on this issue and look forward to working with you as this bill moves forward.

[Additional material may be found in committee files.]

STATEMENT OF COMPUTER-BASED PATIENT RECORD INSTITUTE, INC.

On October 24, 1995, Senator Robert Bennett (R-UT), chairman of the Senate Republican Health Care Task Force, introduced the Medical Records Confidentiality Act of 1995.

CPRI congratulates Senator Bennett for the foresight to introduce legislation that will provide consistent, comprehensive protection for privacy in health care information. Whether in a paper-based or computer-based environment, federal preemptive legislation protecting the privacy of private sector health information with civil and criminal penalties is absolutely essential and long overdue.

The recent OTA report on Protecting Privacy in Computerized Medical Information (1993) highlights that state laws vary in scope and collectively do not afford the protection that is needed under health reform and increasing computerization. As more care becomes managed and there are increasing uses of health information for business purposes, privacy legislation must exist to afford protection against the many harms that may arise out of breach of confidentiality. Among these are loss of employment and housing, health and life insurance problems, and social stigma. As individual health care providers form integrated delivery systems and utilize computer networks to exchange information—often across state lines—federal preemptive legislation will be the only manageable way to govern disclosure of protected health information and provide appropriate sanctions for breaches of confidentiality.

Public surveys (Harris/Equifax, 1993) also support the need for tough enforcement to ensure that gains made by computerization are not lost through adverse confidentiality experiences. Increasingly, the public is concerned with privacy in all segments, of which health is perhaps the most sacred. Computerization can afford better protection against breaches of confidentiality, but these protections must be legislated to ensure they are in place everywhere. Individuals are also becoming much more active participants in their health care and should have not only the right to authorize release of information, but the responsibility for understanding that information through appropriate access and making informed decisions about who may have that information.

CPRI formed for the purpose of initiating and coordinating activities to facilitate and promote routine use of information technology to improve health care quality, cost, and access. Computer-based patient records are not merely automated forms of today's paper-based medical records, but encompass the entire scope of health information. Computer-based patient record systems facilitate the capture, storage, processing, communication, security, and presentation of non-redundant information on a person's lifetime health status and health care, distributed across care sites and providing an enabling partner for caregivers and other authorized users with legitimate uses. Such systems contribute to more effective and efficient health care through universal and timely access to lifetime health data across the continuum of care.

The Computer-based Patient Record Institute (CPRI) grew out of the recommendations of the National Academy of Sciences, Institute of Medicine, report on Computer-based Patient Records: An Essential Technology for Health Care (1991). CPRI is a non-profit organization, with members representing the entire range of stakeholders in the health care system.

STATEMENT OF EVAN HENDRICKS

My name is Evan Hendricks. I'm editor/publisher of PRIVACY TIMES, a bi-weekly, Washington-based newsletter that reports on legal, policy, industry and consumer news in the fields of privacy and freedom of information. I started PRIVACY TIMES 14 years ago. I have been reporting on privacy and FOIA issues for 17 years. I am author of the book Your Right To Privacy (SIUP-1990).

I am also Chairman of the U.S. Privacy Council, an organization consisting of individuals who work on a variety of fronts to foster better practices and policies in relation to the uses of personal information.

History has taught us that an inadequate legislative response to the foreseeable development of a large, database surveillance system will result in high societal costs. These include unacceptably high inaccuracy rates, causing unjustifiable denials of economic and social services, insider abuse of personal data by fraud artists and electronic voyeurs, and a general sense among Americans that they are losing control over their personal information (see the latest survey by Louis Harris).

Another cost is the time and energy that consumer protection officials must devote in responding to complaints from consumers. The growing chorus of complaints ultimately forces legislators to try to cure the inadequacies in the law—a difficult process because the effected parties become much more entrenched.

It is out of my desire to avoid the mistakes of history that I oppose the current medical records legislation before the committee. Although I strongly support a national law to protect patients' privacy, the current proposal, due to inadequacies which I will discuss below, will do more harm than good by legitimizing a large, database surveillance system while leaving Americans without sufficient choices or remedies to retain a satisfactory level of privacy. The kinds of information systems that this bill correctly envisions represent an electronic Goliath that will gobble up sensitive medical data about millions of consumers, while the proposed protections will only equip them with a crude slingshot. My hope is that the bill will be revamped so it will live up to its goal on ensuring confidentiality.

A Case Study: Credit Bureaus

The current medical records proposal in many ways parallels the Fair Credit Reporting Act (FCRA) of 1971. Due to the credit industry's influence, the FCRA inadequately addressed a host of issues, including consumers' rights of access and correction, and civil penalties. The law failed to impose strong enough duties on credit bureaus to reinvestigate and correct errors, deter insider abuse and completely avoided the duties of those that furnished data on consumers. Finally, the law did not create an adequate oversight mechanism.

The results are now in. Independent studies have found high rates of data inaccuracies in credit bureaus. Throughout the 1990s, problems with credit reports have been one of the leading cause of consumer complaints to the Federal Trade Commission. Nineteen state Attorneys General filed a lawsuit against one major credit bureau, TRW, which was ultimately settled. A growing problem now is "identity theft," that is when fraud artists take advantage of their authorized access to credit bureaus in order to steal someone's name, Social Security number and other particulars so they can order credit cards in that person's name and then go on a buying spree. The consumer is only liable for $50, but then must spend hours upon hours trying to convince the credit bureaus that he or she is not responsible for all the unpaid bills.

Congress already has toiled four long years trying to reform the law, but has seen legislative proposals twice "die on the vine." Now with hindsight we can see that much of the damage to consumers, and the time and energy expended by enforcement officials and legislators, could have been avoided if an adequate law was enacted from the outset.

Making This Bill Work

If we continue on the current course, there is every reason to believe that the evolution of America's medical data systems will parallel that of the credit bureaus. Examples of insider abuse of patient data regularly surface. A 1994 survey by Hewlett-Packard showed that only 24 percent of the health care officials responding said they have instituted sign-on passwords and logging of access to highly sensitive computerized patient data. In England, the Audit Commission, which oversees that country's health care system, found that computerization has failed in many cases to provide benefits to patients and has resulted in invasions of privacy.

Accordingly, the following is a list of provisions the current medical records bill needs to make it a medical privacy bill:

Independent Oversight Office. Any law, particularly this one, needs enforcement and oversight. The current proposal vaguely punts some duties to the Dept. of Health and Human Services. But HHS is not up to the job. What's needed is an independent national office, possibly one answering to Congress, like the General Accounting Office. Such an office need not be large, but privacy must be its mission. Nearly every Western nation has an office of this sort. They handle complaints, make recommendations to legislators and, in some countries, can audit data holders to ensure an adequate level of privacy. The bipartisan Privacy Protection Study Commission endorsed such an office in 1976; an HHS Task Force on Privacy endorsed one in its September 1995 report.

Health information Services. The bill gives far too much leeway to HIS. Currently, the bill would allow the most sensitive medical data go into a third party database (medical-style credit bureau?) without the patient's consent. The HIS could then "facilitate the transfer and exchange of" or "authorized access" to this sensitive data, all without the patient's consent. No "privacy" bill would every authorize such sweeping usea of personal data.

Patient Choice. The bill does not give patients any choice or control over what kind of health data about them that can go in a large database. While there are many reasona to facilitate the electronic exchange of billing and other administrative data, the bill fails to distinguish these from some of the super-sensitive information contained in the patient's record.

Law Enforcement/Admin subpoenas. Given the lack of an oversight office, this provision simply gives enforcement officials too much leeway to obtain records without the patient's knowledge.

Patient's Right To Remedy. The preemption of state law is much too broad. The federal law should set a floor for individual rights, not a ceiling on them.

For more detailed comments on how the bill must be revised, please see the testimony of Denise Nagel, Coalition For Patient Rights.

STATEMENT OF LAWRENCE O. GOSTIN

I am the Co-Director of the Georgetown/Johns Hopkins University Program on Law and Public Health with faculty appointments at the Georgetown University Law Center and the Johns Hopkins School of Hygiene and Public Health. I also Chair the Health Information Privacy Project supported by the U.S. Centers for Disease Control and Prevention (CDC), the Carter Presidential Center, and the Council of State and Territorial Epidemiologist (CSTE). I am on the HIV Advisory Committee of the CDC.

The CDC/Carter Center/CSTE "Health Information Privacy Project" is a two year project. The Project has undertaken a national survey of laws and regulations affecting the use, storage, and dissemination of health information. This national survey has been conducted through state health departments and offices of attorneys general. The project has also developed model guidelines for health information privacy that were developed by a multidisciplinary group of experts in public health, research, law, ethics, and community-based organizations convened by the Carter Presidential Center. The final Report of the Health Information Privacy Project is in draft form and is shortly to be published by the CDC.[1] In addition, an article describing some of the reaults of the Project will appear in the Journal of the American Medical Association (JAMA).

The current issue of the Cornell Law Review contains an article on "Health Information Privacy" which systematically examines the compelling public purposes served by collection of health information, the privacy invasions, and the inadequacy of current federal and state law to protect privacy.[2] The article strongly supports a federal preemptive statute on health information privacy. The Cornell Law Review article contains the full reasoning why I support a Bill like the Medical Records Confidentiality Act of 1995. I am enclosing a copy of the article and request that the full contents be read into the record.

Justifications for a Federal Preemptive Statute on Health Information Privacy

A health care system supported by data on almost any relevant subject, accessible to a diverse and significant number of users, is an integral part of the vision for health care in America. Plans for the systematic collection, storage, use, and dissemination of a huge volume of uniform data sets in electronic form are already under way and have an aura of inevitability. This new health information infrastructure is the subject of reports recently published, or in press, by the Congressional Office of Technology Assessment, the General Accounting Office, the National Academy of Sciences, the Department of Health and Human Services, the Physician Payment Review Commission, and the Centers for Disease Control and Prevention.

Powerful reasons exist for the broad collection and use of health data. High quality data are needed to help consumers make informed choices among health plans and providers, to provide more effective clinical care, to assess the quality and cost effectiveness of health services, to monitor fraud and abuse, to track and evaluate

[1] Lawrence O. Gostin, Zita Lazzarini & Kathleen Flagherty, The Health Information Privacy Project: Legislative Survey and Guidelines on State Privacy Laws, with Specific Emphasis on HIV and Immunization (CDC, CSTE, Carter Presidential Center, Atlanta: Forthcoming).

[2] Lawrence O. Gostin, Health Information Privacy, 80 Cornell L. Rev. 451 (1995).

access to health services and patterns of morbidity and mortality among underserved populations, and to research the determinants, prevention, and treatment of disease.

Aggressive collection of a broad range of personal data, however, has a significant trade off in loss of privacy. American society places a high value on individual rights, autonomous decision making, and the protection of the private sphere from governmental or other intrusion. Americans currently believe that their privacy rights are not adequately protected. In a 1993 Harris-Equifax poll specifically on health information privacy, eighty percent of the respondents believed that consumers had lost all control over how medical information about them is circulated and used. Eighty-five percent of respondents said that protecting the confidentiality of medical records is an absolutely essential or very important part of reform of the health care system; they put this priority even ahead of providing universal coverage, reducing paperwork burdens, and providing better data for research into diseases and treatments. Public fear and distrust of technology and bureaucracy are only likely to increase as collection, storage, and dissemination of information becomes more automated.

Health information is perhaps the most confidential, personal, and sensitive of any information maintained about an individual. Currently, government agencies (e.g., defense, law enforcement, health and welfare, and public health), researchers, academic institutions, employers, insurers, commercial marketers, and many others have vast databases of personal health information, often in automated and identifiable form. These data include genetic information that potentially allows the holders of these data to unlock the most deeply intimate details of the past, present, and future health status of the individual and his or her family.

To a great extent collection, use, and transmission of these data are unregulated or underregulated at the federal or state level. The Health Information Privacy Project survey found federal and state law to be inconsistent and highly variable. The Project concluded that extant law was insufficient to adequately protect health information privacy. An ideal federal statute would facilitate the collection and use of health information for compelling health purposes. At the same time the statute would provide reasonable public assurances that the information would be used only where necessary to achieve a substantial health purpose; with the patient's consent (unless the data are in non-identifiable form or where consent would thwart a compelling health objective); and in accordance with principles of fairness, access, confidentiality, and security.

Preemption of State Privacy Law

Continued reliance upon current legal safeguards is incompatible with the policy objectives of an integrated health information system for a number of reasons. A state-by-state approach to regulation of medical information does not reflect the realities of modern health care finance and delivery. The flow of medical information is rarely restricted to the state in which it is generated. Such information is routinely transmitted to other states, subject to differing legal requirements, for a wide variety of purposes ranging from medical consultation and research collaboration to governmental monitoring for quality.

Further, the physical location of health information is no longer relevant. Databases containing huge quantities of personal information provide immediate access to a variety of eligible users in remote locations. Thus, laws that attempt to regulate information physically located in a particular state are ill suited to the need for efficient collection of information and the enforcement of reasonable levels of privacy in a postelectronic era. The prospect for resolving these problems through the enactment of model or uniform laws in every state is exceedingly small. The National Conference of Commissioners on Uniform State Laws adopted the Uniform Health Care Information Act in 1985, but only two states, Montana and Washington, have enacted it.

The absence of a uniform health information policy imposes hardships on virtually all concerned. Health care institutions, insurance companies, and self-insured employers who transmit health data through interstate commerce often do so without clear guidance regarding which state's laws govern or which state's courts have proper jurisdiction to resolve disputes that may arise. Without the ability to know and to rely on uniform regulation of information, patients lack the basis for meaningful consent to disclosure. Lack of uniformity adversely affects the integrity of health data, and the quality of care itself, by undermining efforts to automate health records. Consequently, many persuasive reasons exist to adopt a uniform federal health information policy that transcends state borders.

Critics argue that a preemption strategy does not permit states to create stronger rules of privacy: if a state legislature were to give greater credence to the value of

privacy, it could not act in the face of a preemptive federal statute. While many would not wish to prevent states from giving more rights to privacy than are provided at the federal level, allowing auch state actien would defeat the chief goal of a preemption strategy. By permitting greater protection of privacy, a state would impede the free flow of information across state lines. Thia ia precisely what a preemption strategy would seek to prevent.

Enhancement of Efforts to Computerize Health Information

It is possible to read the Medical Records Confidentiality Bill as somehow creating, legitimizing, or enhancing current efforts to computerize health information. I think, however, that this is a mistaken reading of the Bill. To be aure, the Bill would regulate electr0nic? as well as manual, health data giving the appearance of legitimacy. However, this is a problem (if it is a problem at all) that exists under the current system and is not caused by the Bill. The Institute of Medicine recently observed: "No one engaged in any part of health care delivery or planning today can fail to sense the immense changes on the horizon, even if the silhouettes of those changes, let alone the details, are in dispute. " The Institute was referring to the development of a national health information infrastructure, which I define as the basic, underlying framework of electronic information collection, storage, use, and transmission that supports all of the essential functions of the health care system. In fact, every government and professional review of health information has observed the rapid development of health database organizations collecting and disseminating vast amounts of automated data.

Currently, federal and state law poses little restraint on the activities of these health database organizations, particularly in the private sector. The Bill, while not strong enough in several respects, clearly provides substantial protection for privacy and security where little currently exists.

Authorized Access Under the Medical Records Confidentiality Act

The single most effective method for protecting health information privacy is to empower patients to control their health records: provide patients with (i) relatively unencumbered access to the records to assure fairness, accuracy, and completeness; (ii) a procedure for correction of records; and (iii) the right to grant or withhold informed consent to the disclosure of records. The Bill almost uniformly achieves the first two purposes of access to, and correction of, records.

The Bill achieves the third, and most important, purpose of allowing patients to consent to disclosure in at least three meaningful areas: (i) treatment—all health care services patients receive for diagnosis, prognosis, care, or treatment; (ii) payment—reimbursement for health services rendered; and (iii) purposes other than treatment or payment—I read this to include disclosure to non-health-related government agencies (e.g., immigration, tax, welfare benefit services), employers, landlords, businesses, commercial entities, marketers, and others who are not performing essential health functions. Patients feel most betrayed when their personal information is disclosed without their consent where it will be used for commercial or marketing purposes, or where it can be used in ways that cause embarrassment, stigma, or discrimination. Express clarification (e.g., by providing a non-inclusive list of entities that may not have access to personal data without consent) would create higher public trust in the Bill.

The greatest potential for invasions of privacy and harm in the Bill occur in those areas which do not appear to require the patient's consent prior to disclosure. I discuss some of the areas in the Bill where consent does not appear to be required before disclosure. This is not an inclusive list. For example, serious consideration ought to be given to disclosure requirements to law enforcement in the absence of a warrant based upon probable cause.

Oversight

Oversight agencies frequently have access to data under the current system for purposes of quality assurance, prevention of fraud, financial auditing, utilization review, and other essential health care or health financing purposes. These data are often necessary to achieve these purposes. Patients, however, should be informed that their health information will be used for these purposes. Wherever possible, moreover, aggregate, non-identifiable data should be used.

Public Health

Public health agencies clearly require information about disease and injury for the prevention and control of injury and disease. Certainly, the person's consent is not required where the legislature specifically authorizes the health agency to collect personal data—e.g., mandatory reporting requirements for HIV, child abuse, or gun shot wounds. More importantly, I have complete confidence in public health agen-

cies to protect the confidentiality of personal data. Federal public health agencies such as the CDC and state public health departments have outstanding records in safeguarding patient confidentiality and applying rigorous security arrangements.

The Bill appears to authorize routine collection of a broad range of public health data without the person's consent. It would appear to allow health information trustees to disclose identifiable data for virtually all conceivable activities of public health agencies: authorized, as well as mandatory, reporting, surveillance (broadly construed in the public health literature), investigations, and interventions. These provisions could be strengthened to place the burden on the public health agency to demonstrate, for example, a substantial need for the data, why nonidentifiable data would not meet the need, and why prior consent would be seriously impracticable. The population should be informed if identifiable date were to be disclosed in the absence of consent.

Health Research

The Bill permits trustees to disclose protected health information to a health researcher if a certified institutional review board (IRB) determines that the research project requires use of this information, and the importance of the use outweighs the potential intrusion on privacy. It also requires removal of personal identifiers if it is consistent with the needs of the research project, unless the IRB permits continued use of identifiers.

Two central questions arise about the Bill's research provisions: do they improve on or worsen privacy protections for research subjects that exist under current law? Do they provide as strong a level of privacy as is possible consistent with the imperative of sound health research? Privacy protection for research subjects is contained principally in federal regulations often referred to as the "Common Rule." These rules are applicable to federally funded research and they are frequently followed on a voluntary basis for privately funded research. Additionally, some state statutes regulate research activities within the state. A full discussion of the significant gaps in the protection of data are contained in the Cornell Law Review article.[3]

Current federal regulations, while inadequate themselves for protection of privacy, are arguably stronger than those proposed in Bill. While several categories of research are exempt from the regulations if the data are publicly available or nonidentifiable (e.g., investigations involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens), the regulations do require the IRB to seriously concern itself with issues of confidentiality and consent. In seeking informed consent the investigator must provide the subject with "[a] statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained." The Bill, on the other hand, appears to dispense completely with informed consent to the collection of data and poses a broad balancing test for IRBs to follow. It would be an odd result if the Medical Records Confidentiality Act afforded subjects less privacy protection than those which currently exist for federally funded research.

In addition to dispensing with consent, the Bill also does not place the burden on the investigator to demonstrate: (i) the public health importance and scientific rigor of the study (e.g., could "pro-life" advocates set up a study to review abortion records?); (ii) the need for specific and relevant information (e.g., could the investigator engage in a "fishing expedition" of the entire record?); and (iii) the need for identifiable records (e.g., could anonymous or linkable records achieve the same research purpose?).

The Bill's reliance on the procedural safeguard of an IRB to carry the burden of privacy protection in the absence of strict criteria for consent and disclosure is not warranted by the past records of these boards. There is considerable variation in the rigor with which IRBs review research studies.

Given the acknowledged vulnerability of research subjects, and the documented abuses uncovered in the Tuskegee trial and by the Committee on Human Radiation Experiments, the burden of justification should rest on the researcher, and the IRB should rigorously examine the adequacy of the justifications. For example, the investigator should have to demonstrate: (i) the public health importance and scientific rigor of the study; (ii) why particular information is needed to achieve those purposes; (iii) why the purposes of the study would be thwarted by the use of aggregate data; and (iv) why consent to data disclosure is significantly impracticable. This would be particularly true for release of sensitive data such as reproductive decisions, mental health, HIV, and sexually transmitted diseases.

---

[3] Lawrence O. Gostin, supra. note 1, at 504-505.

Non-Identifiable Data

The Bill wisely considers anonymous data as raising fewer privacy issues. There still remain some areas which could be clarified. To what extent are the collection of human tissue or DNA identifiable? An analysis of the impact of genetic data should be included in the Committee Report. To what extent is group privacy protected? Perhaps some non-discrimination principle and/or procedural review should be required when racial, ethnic, social, or other groups are adversely affected by surveillance or other information gathering. To what extent are linkable data (e.g., identifiable data provided by Medicaid to researchers with scrambled identifiers, but potentially linkable) considered aggregate or identifiable data?

The Bill cannot promise absolute privacy, and it cannot bring us back to a world of complete confidentiality between patient and doctor. But it can assure the public that information will be handled respectfully, securely, and fairly, and that patients will have some measure of control. That, in my view, is a substantial advance in both public health policy and in individual rights. Accordingly, I think there exist powerful reasons to support this Bill while still trying to make it stronger in several respects.

Statement of the American Medical Informatics Association

The Public Policy Committee of the American Medical Informatics Association (AMIA) is pleased to submit this testimony regarding S. 1360, the Medical Records Confidentiality Act of 1995. AMIA applauds the efforts of Senator Bennett, the cosponsors of this legislation, and the Senate Committee on Labor and Human Resources in crafting S. 1360.

AMIA is a 501(c)(3) organization with over 3,600 members, including developers of hospital information systems, medical decision support systems, imaging systems, educational systems, and a broad variety of other applications of computers in medical care. Members include health care practitioners (both creators and users of medical information systems), computer and information scientists, bioengineers, medical librarians, academic researchers, and educators. AMIA serves as an authoritative body in the field of medical informatics and represents the United States in international forums.

In order to protect patients/consumers, health care providers, administrators, and system developers, federal legislation must be passed to address the confidentiality of medical records in both electronic and paper form. The public must feel confident that the information in their medical records is accurate, will be used properly, and will not disclosed improperly by any health care provider, insurer, data collector, researcher, law enforcement officer, etc. In addition, the health care community in a mobile society needs access to medical records information in order to provide better, less expensive, and more effective care to patients, while at the same time protecting confidentiality.

Medical record data is proliferating and crossing state lines every day, not only as patients physically move, but also as medical care organizations and insurers expand from one state to another. State laws governing medical record confidentiality are not consistent and sometimes non-existent. Patients in some states cannot even access their own health care information to check its accuracy. How S. 1360 will supersede or interact with existing state legislation is also an important issue.

Psychiatric and HIV/AIDS information are very sensitive data that are governed by separate laws in some states and should receive special attention in federal legislation. In addition, persons who generate patient records need to be protected because sensitive information in a patient's record is sometimes provided privately by a patient's friends or family. Strong federal medical records confidentiality legislation can both protect the patient's privacy and not be an undue burden on health care providers or users of health care information. In addition, such legislation must provide penalties for persons who misuse or improperly disclose information.

The United States needs legislation that addresses medical records confidentiality that clarifies the use of patient data, especially in the era in which it is inevitable that advanced information technology will be used for managing such data. S. 1360 is generally a good bill. As is true with most early versions of legislation, there are some provisions that need to be studied and discussed further. AMIA is interested in the future of S. 1360, and our members are willing to offer assistance as the Committee marks up the bill, and comments from several of our members is included in the Appendix.

APPENDIX

SPECIFIC COMMENTS ABOUT S. 1360 FROM SEVERAL AMIA MEMBERS

Comments below provided by Seth M. Powsner, M.D., Associate Professor of Psychiatry, Yale University School of Medicine. Dr. Powsner is a practicing psychiatrist and a respected researcher in the medical informatics community.

1. S. 1360 does not appear to mean to relax existing protections afforded psychiatric records by state statutes (SEC.401.c.3 and 6). It would be reassuring if S. 1360 clearly said that psychiatric records were to be afforded at least as much protection as medical records, where no state laws apply. It would make sense if the more stringent rule, state or S. 1360, had effect when there are existing state laws.

2. S. 1360 will not necessarily clarify or simplify electronic medical record keeping. Each medical center has to consider both local statutes and S. 1360 if any psychiatric information is involved. Collaborative projects may have to review state law applying in all states from which patients regularly arrive. Only a state by state review of mental health and medical record statutes, and related case law, will reveal S. 1360's actual impact. Moreover, only future actions of the Secretary of Health and Human Services will determine how S. 1360 affects electronic medical records.

3. SEC.213—The public presumably expects more stringent, not more relaxed standards for "electronic" disclosure. Perhaps text could be added to insure that electronic standards will be at least as restrictive as conventional standards. Also, how should medical record systems segregate prescriptions? (Consider routine antibiotics versus anti-HIV agents, antidepressants for chronic pain versus other psychiatric medications or methadone maintenance.)

4. What becomes of state statutes restricting results of HIV testing and the like? Is that meant to be covered by SEC.401.c.3? Clarification of the term "public health" might be helpful.

5. SEC.301, 302, 311—People want protection from mistakes and inadvertent disclosure of private information. These sections do not seem to cover inadvertent, but embarrassing disclosures. Perhaps a $100 fine would be appropriate. (There was a news item about medical records dropped in an office supply store. It is no reassurance that one could sue after suffering monetary damages.)

6. People want protection from decisions based on medical record systems, not just an option to review and amend their records. Cars come with low oil warning lights, not just dipsticks. The Federal Trade Commission already requires that insurance companies using the Medical Information Bureau (MIB) inform potential buyers when their policy application has been refused because of MIB information. Perhaps S. 1360 could require notification when "private" medical record information leads to insurance or job denial. Free copies of the records used might be appropriate. (And, an explicit limit on copying charges in SEC.101 is necessary to make meaningful a person's right to check their records.)

7. People want protection from technical hubris. The Challenger disaster is remembered by most voters even if the Sloan-Kettering system break-in and publicly reported credit-card information system break-ins are not. All systems are subject to misuse and abuse, yet S. 1360 does not specify requirements for personnel staffing medical information systems, much less requirements for reliability and security of the systems themselves. Only SEC.311.a.2 and SEC.311.a.3 suggest that perhaps people who knowingly disclose information might be excluded from federally funded programs.

8. People want protection from legal Catch-22's. As it currently stands, no one can afford private medical care without medical insurance. No one can get insurance reimbursement without releasing their medical records for insurance review. Most insurance policies are provided through employers, many of whom handle initial claim processing inside the company. So who actually does have "private" medical care? Is there text that could be added to S. 1360 so that one can really believe companies and claims processing personnel will be monitored to prevent disclosure? Neat legal or technical arguments are not helpful. Often people feel forced to sign blanket disclosure authorization forms as they are wheeled into hospital emergency rooms.

9. People want protection from law enforcement agencies no matter how much they are favor of law and order. The wording of SEC.212 seems to allow secret subpoena and review of medical information. This would make medical records like phone calls—subject to secret surveillance. SEC.212.a.5.A raises a theoretical possibility of repeated delays in notifying the affected individual of a warrant. Is this reasonable? SEC.210 does not specify a right to object to judicial or administrative disclosures on any particular ground.

10. SEC.101.b.3.B protects administrative information that "has not been disclosed by the health information trustee to any other person." This presumably means not disclosed to an outside organization, and thus protects hospital peer review records from patient inspection. If not, what provides such protection? SEC.401.C.8 only mentions existing statutes.

11. SEC.101.b.2—Protecting confidential sources may prove problematic when patients assert their right to inspect their own records (SEC.101 a).

12. SEC.201.b.1 limits scope of disclosure based on "Compatibility to purpose". Could this be made more specific? It seems very broad and with any latitude in a disclosure authorization would leave nothing protected.

13. Why not a uniform requirement for recording disclosures? Do references to "treatment" also mean diagnosis, etc.? SEC.112 requires maintenance of record disclosures "not related to treatment." SEC.202.d requires health information trustees "maintain a copy of the authorization [for disclosure of information for treatment or payment]." SEC.211 and SEC.212 do not seem to require a record of disclosures for information disclosed under subpoena. (SEC.210.b.1 requires the person seeking information notify the individual affected.)

14. SEC.212.c seems to leave open a law enforcement agency's responsibility to keep protected information confidential. Information may be revealed to an agency without a subpoena and for reasons not having anything to do directly with the patient. Some text to require minimum disclosure, at least for patients who are innocent bystanders, would help.

15. Could SEC.311 concerning wrongful disclosure be applied to a medical student seminar? Suppose a faculty member relates details of a case to illustrate a lesson? The patient's name is not revealed, but one student guesses the patient's identity. The student later discusses the patient by name while out on a date in a public place. Who is prosecuted? Who is subject to civil action?

16. How are First Amendment rights balanced against individual medical privacy?

Comments below provided by Clement J. McDonald, M.D., Distinguished Professor of Medicine, Indiana University School of Medicine. Dr. McDonald is a member of the Institute of Medicine, a practicing internist, and a past-president of AMIA.

1. Can "disclosure" be re-defined to speak of disclosures outside and inside of a health care providing institution? This clarification would reduce much of the potentially difficult operational constraints that the bill could otherwise impose.

2. Regarding quality assurance, the bill does talk about the peer review processes and explicitly excludes this bill from changing any of that information. However, the current quality assurance processes goes beyond peer review, so the bill might need to be expanded to deal with this issue.

3. The bill would have much less cost and regulatory expense if it took access for direct patient care and billing to be implicit to the provision of care.

4. It might be difficult to require a signature as a condition of giving care because of the coercive aspects. This could put health care providers in a bind that might require them to get permission to use records which they have authored to care for their own patients each time they see these patients. The process becomes more complicated when one considers the transitions that patient data go through in order to complete the care process. For example:

a. Delivery of a lab requisition to a commercial lab and/or the forwarding of lab request information from lab A to lab B because lab A does not do all of the tests requested by the health care provider.

b. Delivery of prescriptions to pharmacies; will the pharmacy have to get permission to use the prescription within its own operation, because the permission from the original care giver did not cover this? What about the passing of prescriptions from pharmacy A to pharmacy B by re-writing one prescription because one drug is not available at the first pharmacy?

c. Information forwarded from a physicians office to a hospital or nursing home when the patient is admitted.

d. Information passed to a consultant when he/she is asked to give advice on a patient.

5. The bill puts many limitations on purpose, person, and duration of access for purpose of treatment and billing, which could cause tremendous problems in day to day care processing. It seems to imply that one must identify particular people or organizations to whom one can pass data for care and billing. That is impossible. One can not know the particular drug store, consultant, lab, hospital, physician colleague who will need to get patient information at the time the signature document is signed. The wording should be changed to permit classes/types of individuals/or-

ganizations to whom the data will be transmitted, with penalties only if the process is abused.

6. Stating absolute time limits seems unrealistic. One could limit by relative time, e.g. for no more than 1-2 years after the last care encounter, except for use to remind the patient of the need for follow up or for preventive care.

7. The requirement for separate forms for permission to use patient data for providing care and billing seems excessive and will add extra expense. The paper cost alone (assuming $.02 per form—a conservative cost) would amount to $20 million assuming 1 billion visits per year. This seems a bit much considering that telling the provider they can not look at the patient data when they provide care is a lot like telling a surgeon you can't look at the operative field when you are doing surgery. Would any patient want that?

8. The requirement for getting permission to use data for research at a non-visit encounter is well motivated, and for some functions, it may be appropriate to require such a separation in time and space. But, if the permission is to use patient information for research purposes, this will add greatly to the cost and practicality of research, if you have to visit patients in their home just to ask them for permission to participate in a research project that required looking at their data. Maybe research requests could be separated some how from other types of data requests outlined in the bill.

9. Access for research purposes may be adequately handled in the bill, but there is some ambiguity. From the contents, one might assume that the requirements under SEC.202 and SEC.203 are not imposed on the requirements of SEC.209. One reason to assume so is that the exclusion of SEC.206—emergency circumstances—could not possibly also satisfy the requirements of SEC.202.

From the point of view of future litigation, it would be best if the relationship between SEC.202 to SEC.209 was more explicit it could be stated that each of the cases are independent. If proper research uses of protected data had to satisfy the requirements of a signature, it would be prohibitively expensive to gather permission to use this data because of the requirements to get information at points in time other than visits.

Further, if the bill is not clear, IRB committees might interpret the bill to mean that everyone had to get permission for any use of protected data.

10. The bill defines research organizations as organizations that are part of academic medical centers. Presumably, this would cover such medical research institutes like the Hughes Foundation and the Regenstrief Institute, but it would be nice to know that tax exempt medical research foundations are covered.

11. The tracking and record keeping requirements could be reasonable or hopelessly expensive for health care systems, depending upon their interpretation. There should be some statement about tracking requirements that are affordable. Whatever is done will add to the cost of health care, and technologic investment must have some relation to the threat we are dealing with, especially while we are trying to save money.

Comments provided by Judy G. Ozbolt, Ph.D., RN, FAAN, Professor, University of Virginia School of Nursing. Dr. Ozbolt is an educator and researcher in nursing informatics with numerous publications and is a member of the AMIA Board of Directors.

1. SEC.202.a.4 and 5 require that the written authorization for disclosure of protected health information for treatment and payment specify or describe the person who is authorized to disclose information and the recipient of information. In providing patient care, physicians, nurses, and other professionals must disclose to one another the information they discover (e.g. medical history) and the information they generate (e.g. treatments performed). Would these actions be covered under the term "described"? It is certainly not feasible to specify by name all of the health professionals who may be involved in a patient's care.

2. SEC.203 "Authorizations for Disclosure of Protected Health Information, Other than for Treatment or Payment" seems to apply to health services research, but is not well designed for health services research. Such research often requires searching through databases of aggregate patient data that may extend back more than one year, yet the authorization to disclose expires after one year (SEC.203.a.4). The impracticality of securing permission to use patient records for such research at a time separate from a health care encounter (SEC.203.a.3) has already been pointed out.

Perhaps the intent is for all health services research to be included under the provisions of SEC.209, "Health Research", but then does SEC.203 still apply?

STATEMENT OF THE NATIONAL ASSOCIATION OF CHAIN DRUG STORES

The—National Association of Chain Drug Stores (NACDS) appreciatea the opportunity to submit testimony on S. 1360, the Medical Records Confideotiality Act of 1995, to the U.S. Senate Committee on labor and Human Resources. NACDS believes that this legislation, with Senator Robert Bennett (R-UT) leadership, moves in the right direction toward ensuring privacy of patient information. However, we have some concerns about S.1360, as drafted. We believe that if our recommendationa are incorporated, this legislation will improve confidentiality of patient data in our increasingly-complicated health care delivery system, will increase overall efficiency in medical information record keeping, and will reduce health providers' costs of complying with multiple-state confidentiality laws.

NACDS includes more than 135 chain companies in an industry that operates over 30,000 retail community pharmacies. Many of our members are multi-state companies. We provide practice settings for the approximate 66,000 chain pharmacists, which comprise the largest single component of pharmacy practice. With retail sales exceeding $60 billion in 1994, chain drugstores represent 72% of the $82 billion retail drug store market. The NACDS membership base fills over 60% of the more than two billion outpatient prescriptions dispensed annually in the United States, one billion through third-party payors. In addition, NACDS membership includes more than 1,200 suppliers of goods and services to chain drug stores.

Comprehensive Use of Electronic Transmission of Prescription Claims

While prescription drugs usually comprise only about 8 percent of a typical health insurance plan's total health expenditures, prescription drug claims usually constitute about 50 percent of total claims volume. Over one billion prescription claims will be transmitted electronically this year. Given this vast number of claims, community pharmacy has been on the cutting edge of incorporating on-line, electronic claims processing into its day-to-day patient care operations. Electronic transmission simplifies the billing process, improves communication with other health care professionals involved in the patient's care, and allows cost-effective delivery of care.

RECOMMENDATIONS TO S. 1360

We have reviewed S.1360 and would like to recommend several clarifications:

Preemption of State Laws

NACDS supports total Federal pre-emption of state health care privacy laws. Chain drug stores that operate in multiple states would find it more efficient and less costly if one Federal standard existed to ensure the privacy of health care information. Many states currently have laws that address patient confidentiality, but often these laws are not consistent and are obsolete because they were written with paper claims processing systems in mind. These conflicting laws lead to expensive compliance costs, as well as possible confusion among health professionals about specific medical record privacy requirements. If Federal confidentiality preemption is not comprehensive, provisions relating to privacy of patient information will continue to vary from state-to-state and compliance efficiency cannot be maximized.

Cost of Compliance Could Be Prohibitive

While we support one Federal patient confidentiality law, implementing the extensive privacy requirements of S. 1360, for which technology has never been developed, could be prohibitively expensive. Under S.1360, many community pharmacies would have to purchase or develop software themselves that would allow the input of required additional patient information. In addition, pharmacists will have to spend additional time during and after patient visits to input required data in the patient profile. A good faith effort should be made through additional hearings to estimate the software costs of complying with these new privacy requirements.

Extension of Effective Date

Given our overall concern about the time needed for software development costs, NACDS strongly recommends that the effective date of this legislation be extended from 12 months after regulations are finalized to at least 18 months. Adequate time must be allowed for software manufacturers to develop their product to include all the pharmacy privacy requirements, to test and distribute the product, and to train pharmacists on product use. The ability of all health care providers to implement this legislation in a timely manner will be critical to successful implementation.

Restricted Access to Personally-Identifiable Clinical Health Care Information

NACDS strongly urges that the legislation make a clearer distinction between those who have access to administrative or financial information about the patient versus those who have access to clinical information about the patient, including patient medication profiles. Access to personally identifiable clinical health care information should only be allowed for health care professionals, such as pharmacists, who are currently engaged in providing health care services to the patient.

State professional practice acts regulate health care professionals within the state to protect the public health and safety. Through licensure of health professionals, the state regulates the scope, qualifications, and nature of professional practice. However, S. 1360 would allow "health information service" corporations to use patient-identifiable clinical health care information to provide services, which is usually limited to those state-licensed health care professionals. This legislation must not preempt state licensure and practice acts.

NACDS strongly urges Congress to amend S. 1360 to prohibit health information service companies, including managed care cost containment administrators, from managing individual patient cases through the use of patient-identifiable clinical health care information. Individual patients must continue to be managed by health care professionals licensed by states to protect their citizens health. Simply putting "on notice" everyone that has access to sensitive patient clinical information that they have a legal responsibility to protect that data is not enough.

Individual patient health care decisions must remain the domain of the patient and the health care professionals, and must not be inappropriately or improperly influenced by cost containment administrators.

Limiting access to patient-identifiable clinical health care information will not impair the ability of managed care organizations to manage health care costs. These organizations will still be able to obtain clinical information, but only after the Patient's name and any other identifiers are removed. Effective use of health care cost containment methodologies, including practice pattern analysis, do not require disclosure of the patient's name or other identifiers.

Provisions Relating Only to Inpatient Facilities Must be Identified

Provisions of the legislation which were intended to apply only to inpatient health care facilities must be carefully identified. Subsequently, it should be clarified that such provisions do not apply to outpatient facilities, such as community retail pharmacies. NACDS suggests that the word "inpatient" be inserted where it was intended so that the provisions of this legislation are not inadvertently extended to outpatient community retail pharmacies or outpatient facilities in general.

Conclusion

NACDS fully supports the overall goals of this legislation, but would like to see the legislation revised to address our concerns. We look forward to working with Congress to help patients feel more confident about the security of their medical records, prohibit health information service companies from practicing pharmacy as described by state law, and to enhance patients' one-on-one professional relationship with their community retail pharmacist.

PREPARED STATEMENT OF CATHERINE S. BAXTER

Chairperson and Members of the Committee: My name is Catherine S. Baxter, and I am the Executive Director of the Medical Transcription Industry Alliance (MTIA). MTIA appreciates the opportunity to present this testimony to the Senate Committee on Labor and Human Resources with regard to S. 1360, the "Medical Records Confidentiality Act of 1995."

MTIA is a nonprofit membership association which represents the concerns of medical transcription business owners throughout the United States. The companies, themselves, are the MTIA members, and the General Member roster includes some of the largest medical transcription companies in the world, as well as companies employing only a handful of full-time medical transcriptionists. Revenues from these companies range from $100,000 per year to just over $50 million.

While the size and revenue of these members varies exponentially, the primary issues and concerns do not. Each medical transcription company and every medical transcriptionist, clerical support person, computer and telecommunications support person, manager, supervisor, and business executive working for that company realizes the awesome responsibility each has to maintain the confidentiality of the identifiable and nonidentifiable health information entrusted to them.

Currently, as pointed out in the hearings before this Committee on November 14, 1995, there are only 34 states which have confidentiality laws, and to further

muddy the judicial waters, record retention laws vary from state to state. MTIA supports and applauds Senator Bennett, Senator Leahy, and the members of the Senate Labor and Human Resources Committee for addressing the need for federal pre-emptive legislation to protect the confidentiality of health information and to assure a patient's rights to access and control the dissemination of that health information.

However, MTIA respectfully requests that Senator Kassebaum and the members of the Senate Labor and Human Resources Committee consider the recommendations of MTIA for the modification and clarification of S. 1360, the "Medical Records Confidentiality Act of 1995."

MEDICAL TRANSCRIPTION AND ITS VITAL ROLE IN HEALTH INFORMATION DOCUMENTATION

To fully understand why S. 1360 is so important to the medical transcription industry, one must first understand the process of medical transcription and the vital role it plays in providing health information documentation to assist in the often life or death decision-making process that ultimately remains the responsibility of the healthcare provider.

In order to put into perspective the enormous volume of data that is processed by medical transcription entities each year, please consider the following information which was provided in part by the American Hospital Association (AHA). During 1990, there were over 92 million emergency room visits, 368.2 million outpatient visits, 11 million outpatient surgeries, 30.8 million hospital admissions and discharges (excluding newborns), and 10 million inpatient surgeries performed.

If each of these events produced only one dictated report, they would generate approximately 543 million documents to be transcribed. If each document contained 50 lines. of transcription (which is a very conservative estimate), over 27 billion lines would be generated. Please note that these 27 billion lines do not take into account consultations, radiology reports, pathology reports, other specialty reports, progress notes, correspondence, manuscripts, dictation by caregivers other than physicians, or doctor's office visits, which collectively add another 27 billion lines.

I would venture to say that the majority of the general population and even many people working in the health care industry could not answer the basic questions, "What is medical transcription and what is the job description of a medical transcriptionist?" The answers to these question were once relatively simple, but technology has transformed this profession almost overnight.

Advances in computer hardware and software technology, digital voice recording and recognition, and telecommunications have all contributed to this rapid metamorphosis. Prior to the late 1980's, medical transcription was carried out primarily using analog voice recordings on cassettes and typewriters or word processors. Today, in little more than 5 years, virtually all medical transcription is being carried out using direct access of digital voice recordings and computers communicating via telecommunications links to networked data repositories.

Today, more and more medical transcription services for healthcare providers are being outsourced to services or individuals who work outside of the hospital. or clinic or physician's office. Hospitals, in particular, do not have the resources and expertise to provide the most up-to-date technology for processing voice-to-text health information documentation. Moreover, they often do not have the apace available to provide for housing the hardware and personnel required to carry out these functions on a 24-hour-per-day basis.

In order to underscore to this Committee the complicated nature and farreaching implications of the current process of medical transcription, please allow me to use the following example. The renown comprehensive cancer treatment center, The University of Texas/M. D. Anderson Cancer Center in Houston, Texas, includes an acute care hospital and an enormous outpatient clinic which sees thousands of patients each week. The transcription of many dictated clinic notes and all hospital reports, including history and physicals, operative reports, consultations, and discharge summaries, is a task currently outsourced to a transcription company based in Maryland. This transcription company, like so many others, contracts with medical transcriptionists who may work in multiple states.

In effect, you have a healthcare provider in one state contracting with a service in another state who in turn contracts to tertiary entities across the country. To say that we need pre-emptive federal laws ensuring confidentiality is an understatement of the obvious.

Regardless of whether the medical transcription function is carried out by employees working inside or outside the healthcare setting or by employees or subcontractors of a health information service, the end result of that transcription process ia

to effect voice-to-text documentation for efficient and effective patient care. In this way, medical transcription does directly impact the cost of patient care by expediting the delivery of that care.

Medical transcription companies and the professional medical transcriptionists who form the backbone of this industry consider themselves vital participants in the healthcare delivery team, and as such we do consider that we are a 'health information service' as defined in S. 1360, Sec. 3, subsection (6, c) and, therefore, a 'health information trustee' as defined under Sec. 3, subsection (7A, i and iii).

Unlike some electronic data interchange or EDI transaction processors, as represented by the Association For Electronic Healthcare Transactions (AFEHCT) at the Senate hearings of November 14, 1995, medical transcription companies and medical transcriptionists do not simply facilitate the "passing of a sealed envelope" of identifiable health information. The transcriptionist produces a text version of the health information from a verbal record that has been dictated by or for the attending healthcare provider, and on rare occasions a text version is created from a handwritten report. At the end of this process of transcription, this document is returned to the originator, the healthcare provider, and with this first generation delivery, the responsibility for the information contained within that document also returns to that healthcare provider.

MTIA'S POSITION

MTIA strongly supports the efforts of Senators Bennett and Leahy and the Senate Labor and Human Resources Committee chaired by Senator Kassebaum to provide federal pre-emptive legislation to mandate strict guidelines to protect the confidentiality of health information and assure the individual's right to access and control the uses and dissemination of their own health information.

Furthermore, MTIA acknowledges that by the very process of transcribing voice-to-text, medical transcription services and individual medical transcriptionists become temporary health information trustees. As a temporary health information trustee, the confidentiality of that protected health information must be protected by continuing education of all participants in the process of medical transcription. Comprehensive security measures should be undertaken, as agreed upon by the healthcare provider and any employee, agent, contractor or health information service, in order to protect the confidentiality of protected health information insofar as it is transcribed and maintained for transmission or first generation delivery to the healthcare provider.

At the point in time of that first generation delivery of a transcribed document, be it complete or incomplete and needing correction or amendment by the attending healthcare provider, the healthcare provider must assume all responsibility for the use, transmission, maintenance, inspection, copying, correction, amendment, disclosure, and accounting for any and all disclosures of protected health information.

If medical transcription companies, and even individual medical transcriptionists, clerical support persons, technicians, and principals of these companies, are compelled by the current wording of S. 1360 to obtain and maintain comprehensive liability insurance, the cost of providing healthcare documentation and creating the substance of the computer-based patient record will become astronomical. Who will suffer the most? The patient whose rights to confidentiality this bill is attempting to protect.

MTIA's position simply stated is that the "responsibility for providing: (1) under Section 101 of S. 1360, inspection and copying of protected health information; (2) under Section 102 of S. 1360, correction or amendment of protected health information; and (3) under Section 112, accounting for disclosures, must remain with the healthcare provider unless, and only upon specific agreement, by contract between the healthcare provider and an employee, agent, contractor, or health information service."

If the current wording of S. 1360 were adopted, a medical transcription company would be considered a health information service and, therefore a health information trustee, who would then be required to allow individuals to inspect, copy, correct, and amend their health information. The language of S. 1360 has farreaching implications for many health information services not represented at the hearings or by testimony, such as coding businesses and offsite storage facilities, who are also health information trustees by definition.

It is also hoped that this Committee will look beyond the provision of confidentiality through federal pre-emptive legislation and realize the global implications of a computer-based patient record.

MTIA is currently an active member of Health Level Seven (HL7) and the American Society for Testing and Materials (ASTM), whose committees on health infor-

mation and the computer-based patient record are working to create standards for the creation, transmission, and storage of health data both within the boundaries of the United States and throughout the world. Indeed, how can we plan for a global interchange of protected health information, when we currently do not protect one individual's right to privacy and confidentiality here within the United States? Let's begin with enacting a well-thought-out, comprehensive federal law that provides guidelines and just penalties for failure to follow the letter of the law.

RECOMMENDED MODIFICATIONS AND CLARIFICATIONS

MTIA respectfully submits the following recommendations for modification and/or clarification of S. 1360:

(1) Section 101 concerning the inspection and copying of protected health information should be modified to exclude a health information trustee who does not provide direct patient care or who does not come into direct patient contact.

(2) Section 102 concerning the patient right to correct or amend protected health information should be modified to exclude a health information trustee who does not provide direct patient care or who does not come into direct patient contact.

(3) Section 112 concerning the accounting for disclosure and the maintenance of that accounting record for 7 years should be modified to exclude a health information trustee or health information service, such as a medical transcription service; an EDI processing service; a coding service, or an record storage facility, which is only a temporary or tertiary custodian of the health information.

(4) The ultimate responsibility for the inspection, copying, correction, amendment, accounting for disclosure, and content of the health record, regardless of the form that record exists in, must reside with the healthcare provider.

SUMMARY

In conclusion, MTIA extends its thanks to Senator Kassebaum, Senator Kennedy, Senator Bennett, Senator Leahy, and the other members of the Senate Labor and Human Resources Committee for addressing this very difficult issue of protecting the confidentiality of health information. In addition, we would also like to thank our strategic partners at the American Health Information Management Association (AHIMA) and their Washington DC representative, Kathleen Frawley, JD, MS, RRA, for hearing MTIA's concerns and acknowledging the need for modification to the existing wording in S. 1360.

MTIA strongly supports the need for federal pre-emptive legislation to protect and secure an individual's health information. We also support an individual's right to have access to any and all health information once it has been authenticated by the healthcare provider and to control the dissemination of that information.

MTIA's members accept the awesome responsibility of providing a secure work environment for processing this confidential health information; however, the responsibility for the content of those health information documents transcribed by any medical transcription entity must rest solely on the healthcare provider who created it or authorized its creation and authenticated its content as being accurate.

Thank you for the opportunity to present our views. MTIA would welcome the opportunity to work with the Committee in the future as this bill moves through what will hopefully be the 104th Congress.

PREPARED STATEMENT OF A. MARIO CASTILLO

I am A. Mario Castillo, a private citizen. I submit this testimony in support of Senate Bill 1360. I am deeply concerned about the inappropriate use of private medical records by commercial data banks and their commercial customers. National standards are needed to control individual health information, protect patient privacy, and insure that there are efficient and inexpensive ways for citizens to correct errors in their medical files. I do not believe that current law adequately protects consumers from commercial misuse of individual medical records.

As a former Chief of Staff of the House Agriculture Committee, I know how important it is to hear the real life experiences of concerned citizens. For that reason, I share with you my current costly and time-consuming experiences in trying to get erroneous and misleading medical information about me excised from the files of MIB, Inc. (Medical Information Bureau) one of the nation's largest commercial data banks.

In 1994, I applied for disability insurance from a number of companies and was rejected by several companies. Upon probing, I found that UNUM Insurance Company of Portland Maine, one of the companies I approached for insurance coverage, had obtained an attending physician's statement (APS) from my physician, Dr.

Bruce Rashbaum, M.D. UNUM's physician misread my doctor's notation of a "hemorrhoid" as a positive "hemocult" (blood in the stool) and filed an erroneous report with the MIB data bank which misrepreaented my medical condition as "colitis, irritable colon, diarrhea, dysentery or enteritis." (Alter considerable effort, UNUM finally retracted its report). Also, UNUM's doctor reported that I had a "disorder of the central nervous system" because, on one occasion. Dr. Rashbaum prescribed sleep medications to facilitate my sleep during one of my world business tripa.

At my request, on December 26, 1994, Dr. Bruce S. Rashbaum, M.D. wrote to the UNUM Life Insurance Company to explain why he gave men sleeping medication prescription and hopefully correct my record:

> . . . to assist Mr. Castillo in sleep because of his business. Specifically he travels all over the world entering different time zones and thia assists him in normalizing his imbalance to the multiple time zones. I professionally feel that this is most reasonable and will also atate what Mr. Castillo has no problem as far aa addiction to any prescription pharmaceutical. I feel that your impreasion that Mr. Castillo requires and utilizes sleep medications regularly is very wrong and a most improper deduction based on my medical records . . .

Despite my doctor's written comments, UNUM Insurance Company refused to delete its erroneous report, amending it to read "general disorder for which there is no specific code."

Thereafter, on August 28, 1995, I again wrote to MIB asking them to remove UNUM's false report from my MIB files. To that letter, I attached a March 22, 1995-memorandum from Doctor Rashbaum which stated:

> Please be advised that Mr. Castillo has been a patient since 1990. He has no pertinent past medical history, he takes no medications on a regular basis, he has had minor surgical procedures, specifically tonsillectomy and wisdom teeth extraction and he does not smoke . . . Mr. Castillo is a healthy, 47-yr-old gentleman who is an excellent risk from a medical standpoint for disability insurance. If I may be of further assistance, please do not hesitate to contact me.

In response to my letter, John H. Dodge, M.D. of UNUM wrote me on September 25, 1995. In his letter, Dr. Dodge stated that he received my August 28, 1995 letter and referenced Dr. Rashbaum's December 26, 1994-letter. However, Dr. Dodge's letter failed to even mention Dr. Rashbaum's March 22, 1995-memorandum and Dr. Dodge admitted to my attorney that "I have not contacted Dr. Rashbaum."

I have engaged legal counsel to represent me in my dispute with MIB and UNUM Life Insurance Company. My counsel has pointed out to MIB and to UNUM, that Dr. Dodge failed to review Dr. Rashbaum's March 22, 1995 letter or to call Dr. Rashbaum, and counsel has again asked for UNUM to retract its erroneous code from my MIB medical records. I await the result of my latest overture to correct my MIB medical record.

Although I have ultimately obtained disability insurance coverage, I cannot stress how much time, energy and money have been spent by me trying to correct erroneous medical information in MIBs data bank.

This is no trifling matter. As I understand it, the negative and misleading information currently in my MIBs file, under current law, may be reported to disability insurance companies for 7 years and reported indefinitely for use in the evaluation of my future application for $50,000 more of credit; a life insurance policy with a face amount of $50,000 or more; or consideration for a job paying $20,000 or more. The fact that I can put a statement in the MIB data bank refuting the erroneous entries of UNUM Insurance Company, is of little consolation.

I am a Mexican American businessman. I travel throughout the world. I have the financial and other resources necessary to ascertain my rights and insist that they be respected. Unfortunately, far too many other minority Americans lack the resources at my disposal. They simply cannot protect themselves from the widespread misuae of private medical information. Consequently, these vulnerable minority Americans, I fear, are often denied credit, life insurance and jobs because of the misuse of their private medical information by commercial data banks and their customera.

Every American citizen, irrespective of aocioeconomic standing, deserves the right to inspect, copy and compel corrections of inaccurate personal records. To date, this has not been my experience. The arrogance of entities auch as MIB, the insurance companies named herein, and individuals auch aa Dr. John H. Dodge of UNUM must not go unchallenged by the Committee and the Congress.

I would be pleased to provide the Committee with supporting documentation from my files and to cooperate with the Committee in any manner necessary as it finalizes this important piece of legislation.

STATEMENT OF THE PUBLIC CITIZEN'S HEALTH RESEARCH GROUP

We are submitting these comments to voice our opposition to S. 1360, the "Medical Confidentiality Act of 1995." Under the guise of protecting the confidentiality of medical records, this bill would promote widespread dissemination of personal, private medical information through the establishment and growth of computerized medical records data banks, and broad access to such data banks by a variety users.

Public Citizen's Health Research Group is a non-profit organization funded by small individual contributions. It was founded in 1971 to fight for the public's health, and to give consumers more control over decisions that affect their health. Among other things, we conduct research and analyses of data obtained from the government and other sources to produce reports to educate the public about important health care issues. In July 1995, we published the fifth edition of Medical Records. Getting Yours, a consumer handbook providing consumers with information on their rights concerning their medical records: how to get copies of records, how to read and understand the records, and how to get mistakes in the records corrected. In the book, we discuss the various state laws governing medical records, and, given the different levels of protection in different states, we agree that a federal law to protect the confidentiality of medical records and to guarantee patients the right to obtain and correct their records, would be an important step in patient protection. This Act, however, does not provide that needed patient protection. While offering some new confidentiality protection, and providing patients nationwide the right to inspect and copy their medical records, the Act as a whole threatens confidentiality more than it protects it.

The stated purposes of this Act are (1) to establish strong and effective mechanisms to protect the privacy of persons with respect to personally identifiable health care information and (2) to promote the efficiency and security of the health information infrastructure so that members of the health community may more effectively exchange and transfer health information. While the bill is entitled the "Medical Records Confidentiality Act," the overall thrust of the bill is to enhance the establishment of medical records data banks and to facilitate the exchange of medical records data among a wide group of users, to the detriment of patient confidentiality, and often without patient consent.

A basic flaw in this bill is its failure to deal directly with one of the most important issues relating to medical records today—the effect of technological advances—both in medicine, and in information technology.

Technological advances in medicine, such as new genetic tests, have expanded the range of information to be found in patients' medical records. With some genetic tests, a person's medical records may contain not only information about their past and current health, but also may contain information about their future health potential—sensitive information that may be used by employers, insurance companies and others to discriminate against the patient based on something that has not yet even occurred.

Advances in information technology, particularly the computerization of medical records, and the ease with which computerized records may be accumulated, analyzed, searched and shared among widely dispersed users, raise critical confidentiality concerns. Today's changes in the manner of medical record storage from an old, paper based system, located in a physician's office, to a modern computerized, "medical records data bank" kept by managed care organizations, insurers, and third parties, means that more privacy protection for medical records is needed than ever before. In spite of the fact that the computerization of medical records is a key threat to confidentiality, the bill does not even mention computers, and only obliquely refers to medical records databanks—a large threat to patient privacy and confidentiality—by using the term "Health Information Service."

In addition to the Act's failure to provide sufficient privacy protection for medical records in the age of computers, the Act also legalizes the widespread use of individually-identifiable patient information, without consent, by a variety of users, including health authorities, health researchers, law enforcement officials, and courts or other parties in lawsuits in which a party's health has been placed in issue. It is difficult to imagine the reasons that such broad access to private patient data is required. Indeed, for much research and analysis of health care issues, aggregate data from which patient identifiers have been removed can provide more than adequate information. Yet, for purposes unexplained except by the most general of terms, such as "public health surveillance" or "public health investigation" or health "research project" by a health researcher, this Act would make available patient medical records without obtaining the consent of the patients involved.

Provisions of the bill that are particularly problematic include:

- Section 207, which provides for disclosure of protected health information with personal identifiers to "health oversight agencies," without limitation on the scope of information disclosed, and with "health oversight agency" being broadly defined as to include agencies engaged in licensing, accreditation or certification of health care providers, or public agencies dealing with compliance with legal, fiscal, medical, or scientific standards relating to the delivery of health care or health care fraud.
- Section 208, which provides for disclosure of protected health information to public health authorities for use in legally authorized public health surveillance or investigation, without any requirement that the public health authorities demonstrate that personal identifiers are necessary.
- Section 209, which provides for disclosure of protected health information, containing personal identifiers, to a health care researcher if a certified institutional review board determines that the information is required for the project, and of sufficient importance to outweigh the intrusion into the privacy of the individual. Thus, personal medical information may be disclosed to thousands of researchers, graduate students, and others, without the patient's consent or desire to participate in the research, and with the only protection offered being the judgment of an institutional review board—one located in the same institution as the would-be researchers, and likely to share the researchers' values concerning the importance of research at the expense of personal privacy.
- Section 212, which provides for the disclosure of protected health information containing personal identifiers to government authorities for a "law enforcement inquiry,"—broadly defined as a violation of, or failure to comply with, any criminal or civil statute, regulation, rule or order issued pursuant to such a statute.

These provisions are but a few examples of the broad disclosure of personal medical information permitted by this Act.

In conclusion, we wish to reiterate our opposition to the Medical Confidentiality Act of 1995. While we support the idea of a federal law to protect medical records, and applaud the sponsors of this bill for raising the issue of medical records confidentiality at a time when it is increasingly threatened by advances in computer technology, this bill fails to live up to its name, and fails to adequately protect the sensitive information contained in all of our medical records.

STATEMENT OF THE AMERICAN PSYCHOLOGICAL ASSOCIATION

Chairman Kassebaum and distinguished members of the Labor and Human Resources Committee, the American Psychological Association (APA), the largest membership association of psychologists with more than 132,000 members and affiliates engaged in the study, research, and practice of psychology, appreciates the opportunity to submit this testimony regarding S. 1360, the "Medical Records Confidentiality Act of 1995," for the record. The APA commends Senator Robert F. Bennett for introducing this important legislation and thanks Senator Bennett and members of this committee for your efforts to protect the confidentiality of patient records.

The APA views the particular importance of S. 1360 as being its protection of the confidentiality of patient records when such records are shared for purposes other than when related to patient care. Rapid changes in the health care delivery system have meant that parties other than health care providers have access to patient records for a host of reasons, including those related to payment for and financial review of services. Technological advances in record-keeping now permit computerized and electronically transferable patient records. While federal and state statutes and case law have generally established the duty of health care providers to protect the confidentiality of patient records, the duty of many third parties must still be legally defined. Therefore, the efforts of Senator Bennett and members of the committee are vital now, at a time when technology and rapid changes in the health care delivery system have resulted in less patient and provider control over the distribution of records to third parties.

The APA believes that S. 1360 is an important effort to protect confidential information in the era of electronic patient information exchange, but the bill can and should be improved. We offer the following suggestions, which we will discuss in some detail.

I. People seeking and receiving mental health treatment have different, often greater, privacy and confidentiality needs regarding their records than persons receiving general health services. The committee should recognize this different need, by ensuring that all state and federal laws that specifically address or impact the confidentiality of mental health treatment are not preempted by the

bill and by clarifying the application of certain language in S. 1360, as currently drafted.

II. While S. 1360 generally provides that patients may object to unauthorized disclosure of confidential information as permitted in the bill, we would suggest that, in certain circumstances, the unauthorized disclosure is unnecessary. Where unauthorized disclosure is necessary, the patient's ability to object should be strengthened.

III. S. 1360 takes an important step towards recognizing that, in our health care system today, many entities besides the patient and his or her treating provider, have access to the patient's records. The bill should offer greater protection to patient records when disclosed for an administrative or other purpose not related to patient care.

It is our intention that our discussion of S. 1360 in this testimony will raise the awareness of Senator Bennett and of the members of this committee, that the bill requires some amendment as it applies to mental health records. We hope that members of the committee and Senator Bennett will look towards APA for further clarification of these issues and for help in improving and strengthening the bill.

I. People seeking and receiving mental health treatment have different, often greater, privacy and confidentiality needs regarding their records than persons receiving general health services. The committee should recognize this different need, by ensuring that all state and federal laws that specifically address or impact the confidentiality of mental health treatment are not preempted by the bill and by clarifying the application of certain language in S. 1360, as currently drafted.

S. 1360 generally provides the same protections for all patient records, whether the records concern mental health or general health treatment. In reality, there exist significant differences in the confidentiality needs of patients receiving mental health services and patients receiving general health services, as has been recognized in statute and by our judicial system. We use the "next of kin" permissible disclosure (section 205) and the provisions permitting patient inspection and copying of their records (sections 101 and 102) as two examples of how S. 1360 does not treat the confidentiality of mental health records differently from patient records for general health when it is necessary and appropriate to do so.

A. Confidentiality, as recognized in law, is central to the psychologist-patient psychotherapy relationship.

Through psychotherapy, psychologists successfully treat a wide range of mental health and substance abuse disorders, ameliorating patient suffering and helping patients to lead more productive and functional lives. Psychotherapy improves our society in innumerable ways, such as by lowering crime, improving worker productivity, and advancing various social relationships.

If persons in need of psychotherapy perceive that communications with their psychologist are not confidential, then they are less likely to seek treatment or to trust the psychologist or to confide intimate and possibly embarrassing issues. The importance of confidentiality between a psychologist or other psychotherapist and his or her patient has been well-stated by our judicial system. The United States Supreme Court indicated (in promulgating a proposed rule 504 (recognizing a patient-psychotherapist privilege), to the Federal Rules of Evidence): that the capacity of a psychotherapist to help a patient is completely dependent on the patient's willingness and ability to talk freely. In order to successfully treat the patient, the psychotherapist must be able to assure the patient of the confidentiality of their communications. 28 USCS Appendix, Federal Rules of Evidence, Rule 504, Appendix 6, pp. 475-478.

States have also recognized the importance of confidentiality in the psychotherapist-patient relationship. In California, by way of example, the psychotherapist-patient privilege is considered a broader privilege than the physician-patient privilege. California Evidence Code section 1014 states that a "patient, whether or not a party, has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication between patient and psychotherapist" The section 1014 psychotherapist-patient privilege "provides much broader protection than the physician patient privilege." Cal. L. Rev. Comm'n Comments, Evid. Code Ann. at 194-195 (Deering, 1986). Unless "a patient . . . is assured that [intimate and embarrassing details] will be held in utmost confidence, he will be reluctant to make the full disclosure upon which diagnosis and treatment . . . depends." Id.

The Supreme Court of California has acknowledged the need for near-absolute confidentiality in treatment, as well as the benefit to society of encouraging potentially dangerous persons to seek treatment. See, e.g., People v. Stritzinger 34 Cal.

3d 505, 194 Cal. Rptr. 431, 435 (1983); Tarasoff v. Regents of University of California 17 Cal. 3d 425, 459-460, 131 Cal. Rptr. 14, 39-40 (1976); In re Lifschutz, 2 Cal. 3d 415, 437, 85 Cal. Rptr. 829, 843-844 (1970). California courts, because of the social and legal importance of the psychotherapist-patient privilege, have consiatently held that exceptions to this privilege apply only in "narrowly circumscribed situations" where "the government seeks to promote a compelling interest and where there is no less intrusive means of accomplishing its purpose." Scull v. Superior Court, 206 Cal. App. 3d at 791, 254 Cal. Rptr. at 27 (1988).

B. Disclosure to "next of kin" and patient inspection and copying of records present two clear examples of the need for S. 1360 to recognize that mental health records require protection that is different from that provided general health records.

Permissible disclosurea to "next of kin" in the bill, if enacted, would considerably weaken the protections afforded to mental health patients in several jurisdictions. Presently, under the laws of several jurisdictions, disclosure to "next of kin" is prohibited absent patient consent. Section 205 does not require patient authorization, as atated in section 203(e), and shifts the burden to the patient to "object to" the disclosure, if deemed by the patient to be unwanted.

While next of kin disclosure contained in S. 1360 appears adequate to protect patienta receiving general health services, such as without authorization informing an unconscious patient's family, that the patient is in surgery, we are seriously concerned that this provision is inadequate to protect the confidentiality interest of a patient receiving mental health services. We recognize that, in certain circumstances, notification of family members is beneficial to both the patient and family and should be encouraged. However, there are other circumstances where disclosure would work at cross purposes with the patient's treatment. Persons who are receiving mental health services as a result of or related to difficulties in their family or other close personal relationships must be absolutely assured of confidentiality in relation to these individuals. Otherwise, these individuals will not speak openly in treatment, resulting in less than optimal treatment results, if they seek treatment at all.

A second concern with the bill's next of kin disclosure is that for patients receiving mental health services, subsection (a)(1)(B) permits disclosure of information if the individual "is not competent to be notified about the right to object." Some statea require, in the least, that the individual's guardian must consent to disclosure of the information.

For example, North Carolina, through its "Mental Health, Developmental Disabilities, and Substance Abuse Act of 1985," requires that a patient or his "legally responsible person" must consent in writing to disclosure of patient information to next of kin. Disclosure, once permitted, is limited to information concerning diagnosis, prognosis, and medications prescribed. To receive additional information, next of kin must submit a request in writing, which is reviewed by the treating professional. The patient's or legally responsible person's consent is likewise required for such additional information. (N.C. Gen. Stat. section 122C-55 (1995))

The APA recommends that section 205 be reconsidered, and at minimum, that language similar to North Carolina and state laws requiring guardian consent for incompetent patients be incorporated into the section.

Sections 101 and 102, permitting patient inspection, copying, amendment, and correction of records offer a second example of the need to treat mental health records differently from general health records. The patient rights to inspection, copying and amendment of their records aeems consistent with the evolving legal recognition of a patient's right to inspect and correct his or her medical record. The language should be further refined to recognize and permit an exception in those inatances, where review of records by a person receiving treatment for mental illness, may be psychologically harmful to the patient or detrimental to the patient's course of treatment.

For example, if a patient suffering from paranoid delusions, who believes he or she is hearing voices, inspects and reads in a therapist's record that the therapist auspects these voices are auditory hallucinations rather than "real" voices, distrust of the therapist could occur, if revealed too early in the course of therapy. In addition, issues of correction of the patient record as provided by the bill are much more complicated for mental health records where there may not always be a clearly correct answer. Again, in the example of a patient suffering paranoid delusions, the client may wish the therapist to correct his or her opinion that the voices heard by the client are hallucinations. Thus, a conflict between patient and therapist is created that may adversely impact treatment or be harmful to the patient.

To protect patients from potential psychological harm, the APA suggests that S. 1360 must specify stronger protections regarding patient access to mental health records than those provided for other general health records. Additionally, the APA recommends that the bill specifically recognize that state laws which are more protective of access to mental health records are not preempted.

In our opinion, the next of kin permissible disclosure and patient inspection and copying of records are just two of perhaps a number of provisions in S. 1360 that should be reexamined to consider their potential impact on the confidentiality of mental health records. The APA would appreciate the opportunity of assisting the committee in examining and improving the application of the bill's provisions to mental health services.

C. The exception for state "mental health" laws from the bill's preemption of state laws should be clarified to include all state laws that currently protect confidential communications between psychotherapists and their patients.

We have discussed the need in this proposed legislation to treat mental health records differently from general health records. In part S. 1360 has acknowledged this need by excepting from its state preemption, state "mental health" laws that prohibit disclosure otherwise allowed under the Act. The APA views this "mental health" preemption exception as vitally important for persons requiring treatment for mental illness and substance abuse.

The mental health exception to state preemption means that state laws across the nation that have addressed with specificity confidentiality issues concerning mental health records will not be preempted. Illinois, by way of example, contains a strong mental health records confidentiality law that should not be preempted by S. 1360.

The Illinois "Mental Health and Developmental Disabilities Confidentiality Act," 740 ILCS 110/1 et seq., specifies requirements for a number of mental health confidentiality issues that are not addressed in S. 1360. We outline a few of these specific requirements below:

- Personal notes of a therapist and psychological test material are not subject to discovery in a judicial, administrative, or legislative proceeding.
- Persons under 18 years of age may be assisted at their option, without charge, in interpreting their patient records upon inspection.
- A state government agency may have access to the records of a disabled person who resides in a developmental disability or mental health facility and who does not have a guardian for the purpose of advocating for the disabled individual in relation to a complaint against the custodial facility.
- A developmental or mental health facility director who has reason to believe that a criminal violation or serious accident has occurred in the facility must report the violation or accident to appropriate law enforcement and investigating agencies.

The APA strongly endorses inclusion of an exception for mental health laws from state preemption in S. 1360. We suggest, however, that the term "mental health" law is ambiguous and therefore recommend that this exception should be clarified so that all state laws, whether or not they could be classified as "mental health" laws, are not preempted on enactment of S. 1360. In addition, the bill should specify that states not be precluded in the future from offering stronger confidentiality provisions, which they might seek to enact.

The term "mental health" law is ambiguous. In many states currently, a range of laws afford patient confidentiality protections for persons receiving mental health services which might not be expressly considered "mental health" laws. Therefore, the APA recommends that the "mental health" preemption exception be amended to include the various state laws that speak to the confidentiality of mental health records but which may not otherwise be expressly considered "mental health" laws.

For example, the psychologist licensing laws in several states specify confidentiality requirements for psychologists. In Illinois:

> No clinical psychologist shall disclose any information he may have acquired from persons consulting him in his professional capacity, to any persons except only: (1) in trials for homicide when the disclosure relates directly to the fact or immediate circumstances of the homicide, (2) in all proceedings the purpose of which is to determine mental competency, or in which a defense of mental incapacity is raised, (3) in actions, civil or criminal, against the psychologist for malpractice, (4) with the expressed consent of the client, or in the case of his death or disability, or his personal representative or other person authorized to sue or of the beneficiary of an insurance policy on his life, health or physical

condition, or (5) upon an issue as to the validity of a document as a will of a client. (225 ILCS 15/5)

If the Illinois psychologist licensing law is not considered a "mental health" law for purposes of S. 1360, then the bill would require Illinois psychologists to violate their licensing law, because S. 1360 requires disclosure in instances where the Illinois licensing law would prohibit disclosure.

Several states now impose on psychotherapists and other providers a "duty to warn" others of potential harm from their dangerous patients. This is another widespread type of state law that is not expressly labelled "mental health" law.

These "duty to warn" laws began in California, therefore California offers a good example of a state that has specifically defined the scope of a psychotherapist's duty to warn and how to discharge it. Through Tarasoff v. Board of Regents of the University of California, 551 P.2d. 334 (1976), and its progeny, California has imposed a duty on a psychotherapist, once the therapist determines that his or her patient poses a serious danger to a third parry, to protect a "readily identifiable victim" from the danger. This protection includes warning the potential victim of the danger, notifying the police, or taking other such actions which breach patient psychotherapist confidentiality.

In the nearly two decades since the Tarasoff decision, several states have come to adopt the Tarasoff or a similar requirement. Many of these laws are related to evidentiary privilege and the abrogation of such privilege for Tarasoff situations.

Section 206 of S. 1360, permitting disclosure of patient information in "emergency circumstances" when necessary to protect "an individual from serious, imminent harm," will undoubtedly impact and potentially preempt the Tarasoff related laws currently enacted in several states, affording virtually no guidance to providers for the balancing of their duty to protect third parties with their duty to protect the confidentiality of communications with their patient.

Therefore, with respect to Tarasoff laws, the APA recommends that the "mental health" exception to state preemption be amended to include this body of law. Additionally, the "emergency circumstances" exception permitting disclosure under section 206, should be narrowly tailored so as not to have ramifications for a range of confidentiality issues that psychologists face, such as those related to Tarasoff-type situations.

II. While S. 1360 generally provides that patients may object to unauthorized disclosure of confidential information as permitted in the bill, we would suggest that, in certain circumstances, the unauthorized disclosure is unnecessary. Where the unauthorized disclosure is necessary, the patient'a ability to object should be strengthened.

S. 1360 requires patient authorization for disclosure of confidential records, except in limited circumstances where confidential information may be disclosed without patient authorization, as provided in sections 204 through 212. These sections of S. 1360 provide that patient authorization is not required for disclosure: (1) related to the creation of nonidentifiable health information, (2) to next of kin and for directory information, (3) in emergency circumstances, (4) to a health oversight agency for an oversight function, (5) for a public health function, (6) related to health research, (7) for judicial and administrative purposes, (8) related to non-law enforcement subpoenas, and (9) related to law enforcement activities.

The APA contends that disclosure of patient records absent authorization should only be permitted in those few circumstances where the need for disclosure is so critical as to outweigh the confidentiality interests of the patient. Importantly, in those few circumstances where unauthorized disclosure is absolutely necessary and appropriate, S. 1360 should place the burden on the holder of the information to have the patient authorize the disclosure. If any circumstances exist where it is inappropriate or impossible to obtain patient authorization, S. 1360 should provide provisions affording patients a strong ability to object to the disclosure, such as, where possible, permitting the patient to object before disclosure is made.

The APA recommends that members of the committee consider the unauthorized disclosures permitted under S. 1360 by the standard outlined above. For instance, we believe that a patient's right to object to disclosure pursuant to a law enforcement warrant (section 212) may be inadequate when the warrant is issued ex parte. When a court issues a warrant ex parte, the patient has not been given the opportunity of offering arguments against disclosure before disclosure.

We believe that through close examination of the unauthorized disclosures permitted in the bill, members of the committee will likely determine that some disclosures are unnecessary, should require the holder of the information to seek patient authorization, or should afford stronger patient objection provisions. The APA would appreciate the opportunity of assisting the committee in reexamining the unauthor-

ized disclosures, particularly as they apply to persons receiving mental health services.

III. S. 1360 takes an important step towards recognizing that, in our health care system today, many entities besides the patient and his or her treating provider, have access to the patient's records. The bill should offer greater protection to patient records when disclosed for an administrative or other purpose not related to patient care.

In our health care delivery system today, many individuals and entities other than the patient and his or her treating provider, have access to patient records. Not long ago, such third party access was not possible. Now it is the norm.

S. 1360 permits third party access to patient records for a number of administrative purposes that are may not be related to patient care. We believe that the bill is not clear, as currently drafted, as to those purposes that constitute "administrative" purposes for permitting disclosure of patient records. Therefore, we suggest that "administrative" purposes be clearly defined in the bill. We additionally suggest that disclosures for administrative purposes should receive closer scrutiny than those disclosures related to patient care.

S. 1360 should strictly limit and regulate such third party access to patient records for two reasons. First, third party access to patient records does not generally directly aid in the treatment of the patient. Such access is beneficial to other parties but not necessarily the patient. Therefore, when confidential information is disclosed regarding a patient for the benefit of third parties, the patient should be afforded a stronger right to restrict access.

Second, third party access often means that several individuals see and use confidential information. Before such third party access became a common occurrence, only the patient and his or her provider shared the information, with limited exception. Today, third party access means that insurers, utilization reviewers, hospitals, and other large entities, allow employees and others access patient records. Thus, it is through the administrative functions of third parties that have weakened the confidential status of patient records.

The APA believes that the inclusion of "health information services" (services) in the "health information trustee" (trustee) definition provides for an important patient safeguard. Such services should be held accountable, as are other trustees, for violations of the confidentiality requirements of the bill. Although services do not provide direct patient care, they do have access to and control patient records. Therefore, S. 1360 should recognize and impose legal standards, as appropriate, for the handling of confidential records by such information services.

While inclusion of services in the trustee definition is an important patient protection, S. 1360 should be amended to remove any access to patient records for an administrative purpose that is unnecessary. In addition, any provision of the bill that inappropriately weakens a patient's rights regarding the confidentiality of his or her records for an administrative purpose should be removed or strictly limited where possible.

The APA appreciates the efforts of Senator Bennett and members of the Senate Labor and Human Resources Committee in seeking to protect communications between a patient and provider in this new era of electronic databases and release of information for purposes other than that related to patient care. The APA believes that S. 1360 represents an important step towards protecting the confidentiality of patient records but requires revision to ensure that privileged patient-provider communications are adequately and appropriately protected.

We hope that this testimony raises some constructive considerations for improvement of S. 1360, particularly as it would apply to the confidentiality of mental health records. We look forward to working with Senator Bennett and members of this committee to improve and pass this important legislation.

STATEMENT OF MARY G. BONK

COGS (Complications of Gynecologic Surgery) women's support group was formed in 1985 for the purpose of finding and communicating with women who have had untoward complications of gynecologic surgery. Limited documentation of identification, symptoms and medical history is preserved.

Of primary Interest are unresolved problems of hysterectomy. We believe that present federal health policy protects surgical abuse of women by the withholding of diagnosis and information of certain complications of hysterectomy.

This testimony will focus on the unresearched and undocumented gastroenterological complications of hysterectomy.

Specific complications, mechanical in definition, some spontaneous and others over a period of time, present pain and major dysfunction. The woman'S search for

evaluation, information and medical help is progressively unproductive because certain mechanical complications of hysterectomy cannot be surgically addressed with vaginal presentation.

All information is withheld, and abnormal and pathological functioning of the digestive and excretory organs evolve into progressive and inevitable digestive disease.

Over the past 6 years COGS has documented numerous female citizens who are refused medical assessment, diagnosis and helpful treatment throughout the US. Specific and serious disorders of digestive disease are evidenced by their physical complaints, indicated by their medical history and documented by xray films and other data.

Psychiatric referral is the common route of treatment.

Psychiatric manipulation has been used to suppress diagnosis of physical disorder and has substituted psychiatric illness as reasons for complaint or dissent. The affected woman cannot exhibit dysfunction or prove her chronic pain; she only knows that it has been caused by surgery. There is loss of credibility, family support, self image and emotional stability.

We believe that loss of hope for help often results in institutionalization or suicide of these women.

Health research in this area of women's health care has been politically suppressed. Imposed conspiring within the scientific community has involved unpublished diagnostic codes, undocumented and misleading health reports, incomplete patient operative records and charts and fraudulent withholding of evident and diagnosable conditions.

The Commission on Digestive Disease, Public Law 94-562, created by the 94th Congress, Oct. 19, 1976, consisted of over 500 members which included possibly only two female medical doctors. The Report to Congress of the U.S. of this Commission in 1979, DHEW Publication No. NIH 79-1878 did not address digestive disease which results from prolapse, outlet obstruction or other complications of hysterectomy which cause intestinal or rectal dysmotility.

Toxic megacolon, megarectum, enteroptosis, irritable bowel syndrome, diverticulosis, aganglionosis, ostomies, pernicious anemia, pathological changes in blood chemistries and other non-absorptive syndromes, colitis, intestinal rupture, rectal ulcer/cancer, colon ulcer/cancer, fecal and urinary incontinence, and erosion and malignancies from the use of foreign materials such as Ripstein, Nigro, Corman and Thiersch surgical procedures, have not been indicated by women's health research as gastroenterological complications of hysterectomy.

There has been uncontrolled surgical experimentation on women in this area of health care throughout this century. Numerous surgical procedures, harmful and sometimes bizarre, are described in medical papers and books such as Goligher's Surgery of the Colon, Rectum and Anus. Many of these experiments have been done on patients in mental hospitals and some during the last decade in veterans' hospitals in South Carolina. Many are unproposed to the patient and undocumented. Comprehensive or long term results, as well as the incidence of their use, seem to be unpublished. Results are measures as "successful" or "unsuccessful" and many patients are "lost to follow up".

The gastroenterological assessment of these specific initial complications of hysterectomy, the long term effect of the untreated condition or the undocumented and/or secret remedial surgical procedures are not within current federal health policy.

Documentation and confirmation of digestive disease which results from complications of hysterectomy, early and late, would markedly reduce the national rate of 700,000 hysterectomies per year.

Uncomplicated and well researched procedures of gastroenterological investigation of these conditions are described in Coloproctology and the Pelvic Floor, Pathophysiology and Management, Butterworths, 1985, by Henry and Swash. This work was centered at St. Mark's Hospital, London, UK and done by world leaders in this area of medical science. 28 European and 8 American physicians and surgeons contributed to this book.

It Is important that research procedures be established for the defining and documenting of gastroenterological pathophysiology which has genesis in hysterectomy. It is imperative that women who are presently in chronic pain, dysfunction and progressive disease be rescued by appropriate scientific evaluation and options for open and ethical surgical relief.

Personal health care account

I am a currently registered nurse but have not been employed since 1983 because of the diaabling condition herein described. I am 61 years old, married for 39 years and have 4 children.

After a vaginal hysterectomy in 1979 for aymptomatic cystocele, I experienced localized positional pain above the navel at 2 weeks post surgery. There was aevere vaginal tightness, itching, and amall amounts of bright bloody discharge. There waa also dysfunctional defecation for the first time in my life.

At 4 montha post hysterectomy and after employment related compulsory recertification of CPR, a new range of abdominal discomfort, pain and dysfunction appeared. Medical doctors' who were consulted for diagnosis and information during the next 2 years included the gynecologist who did the surgery (numeroua timea), our primary doctor of internal medicine, a general surgeon and three other gynecologists. All information was withheld.

In 1981 a colon and rectal surgeon did what I believe to be harmful, unproposed and undocumented surgical procedures and abandoned me in pain and dysfunction.

Upon returning to the gynecologist who had referred me to the colon and rectal surgeon, his advice was that I should "go to some big medical center". When I left his office he said "you won't find any help anywhere in this country".

Sleeplessness, pain and panic drove me to be admitted to a mental health center where a psychiatrist told my husband that he might have to administer electroshock therapy. That I was aeriously ill. After a full night's sleep from one dalmane I resolved to be obedient, observing, and ask for early discharge and aeek medical help in another area of the US.

After 4 days I was discharged and I returned to part time registered nurse duties at a general hospital the next week after discarding the psychiatric drugs which were prescribed.

With my husband I aought gynecological consultation in another atate, and from this appointment found a vaginal surgeon in the Northeast. Although this surgeon gave me no information, I perceived that relief and resolution might be possible. And from this hope I have averted suicide.

We have paid over 50 medical doctors in 8 states of the US and have sought medical assessment and surgical relief in 5 highly reputable university medical centers and clinics. All information is withheld.

We have appealed to medical societies and licensing boards in two states.

I have filed Civil Action No. D-8980 in Fulton County, GA in order to depose a diagnostician whom we had paid for examination and tests but would give us no information. He was a hostile witness who withheld all information again and would not sign the document of deposition.

After extensive research in Emory Medical Library I am convinced that specific Surgical procedures were used which cause me chronic pain, dysfunction and progressive disease. But they are undocumented.

I believe that during hysterectomy in 1979 there was vaginal suspension to the right round ligament which predisposed mesenteric displacement by traction, ptosis of the small bowel, sigmoid and transverse colon.

Other undocumented surgery suspected done in 1981 was: rectosigmoid resection with proctopexy and colopexy (Frykman Goldberg and Pemberton-Stalker ?), usage of foreign body such as Thiersch silastic circlage with suspension, that levator muscles were surgically changed (Graham?), fixation of the urinary bladder to the pelvic abdominal wall, vaginal auspension to the left pyriformis muscle causing extensive tissue changes at the femoral joint, sacrum and vagina with chronic spasm and damage to the puborectalis muscle which is necessary for continence.

I am in possession of over 100 xray films which by our research provide basis for this suspected undocumented surgery and the results of such. But I am denied aasessment throughout the nation, including doctors, (radiologists, etc.) who serve as experts for attornies. I am thrown away by science and law.

We have been to Ontario, Canada (1986) and London, England,(1987) to have investigative procedures as published by world experts in Coloproctology and the Pelvic Floor. The results of these tests which were not available to me in the US were aent to a diagnostic authority in Maryland who does not asaess them, assumingly because this would violate current federal health policy. (Since independently arranging consultation with this authority at Francis Scott Key Medical Center in 1985, he has held results from all medical investigative procedurea done in the US, Canada and England.)

In August 1988 Civil Action No. R-88-2234 waa filed in US District Court in Baltimore, MD against this diagnostician in effort to obtain information. This physician could not be subpoenaed for a hearing on September 1, 1988. A protective order opposing the patient's request for deposition and production of documents was honored

by federal judge Norman T. Ramsey, who dismissed the complaint by summary judgement on September 30. He would not allow the plaintiff to obtain oathed procedure of the diagnostician who never appeared.

Since May 1987 communication concerning this area of federal health policy has been attempted with Senator Edward M. Kennedy, Chairman of the Senate Committee on Labor and Human Resources.

By multiple letters, 1988 through 1990, we have presented a petition for hearing concerning this area of federal health policy to members of the House Committee on Energy and Commerce. Support for this inquiry was personally requested from 25 female US Representatives and 2 female US Senators at their Washington offices in 1989.

After denial of request for hearing by the Chairman of the Health Subcommittee in March 1990, a new petition for hearing, xray films and other data were forwarded to the Senate Committee on Labor and Human Resources by Senator Mikulski in June 1990.

There has been no positive response.

we request that this Task Force on Opportunities for Research on Women's Health obtain all health care information including letters, opinions, personal recommendations and other data concerning this petitioner from Dr. Marvin M. Schuster, world authority on colonic motility and dysfunctional digestive disease.

We request also that further available comparative and comprehensive investigational procedures be employed upon this petitioner for the purpose of establishing research protocol concerning the prevention of certain digestive diseases which are related to dysmotility.

In conclusion, uncontrolled surgical experimentation on women must be replaced by controlled, scientific and humane research in Obstetrics and Gynecology.

And this new science with humanity for all people must take birth at our National Institutes of Health.

STATEMENT OF NAN HUNTER

I am Nan Hunter, Deputy General Counsel, U.S. Department of Health and Human Services. I am presenting for the record our views on S. 1360, which would establish a Medical Records Confidentiality Act.

The topic is vitally important. We are pleased that you share our vision for careful, respectful treatment of health information. Personally-identifiable health information is. used for many purposes to benefit individuals and for broader societal needs. The challenge in legislating rules for confidentiality is always how to strike the best balance between those purposes and the rights of individuals. Let me begin by discussing the factors which underlie our concern for protecting health information.

I. BACKGROUND

The Reasons for Confidentiality

The primary goal of confidentiality in health care is to permit patients to be totally frank about facts which bear on their health, and to subject themselves to examination and tests which reveal facts about them. Without confidentiality protection, sick people would be faced with having to choose between revealing information to obtain treatment, or retaining their privacy—a cruel choice, and one that would in some cases lead to untreated disease, or falsified information.

In public health and research there are equally pressing reasons:we want the patient to be frank not only for his or her own sake, but also for the health of society more generally. Only if we keep the patient's confidences will he or she be candid about sensitive matters. This permits us to intervene to protect others and interrupt the spread of communicable disease, and to gather accurate information to elucidate the causes of disease, evaluate treatments, and understand how the health care system is working.

Legal Protections

Legal protections for health-care information today are skimpy and uneven at best, as the subcommittee is aware. They exist primarily at the state level, and they vary greatly. A few states have comprehensive health-care information confidentiality statutes, including two (Montana and Washington) which have enacted the Uniform Health-Care Information Act of the National Conference of Commissioners on Uniform State Laws. Many have statutes covering particular types of information (like HIV related infection and mental health information), and some have statutes covering insurance information, including health information about beneficiaries. In addition, there is some case law establishing confidentiality duties.

The physician-patient privilege (which most states have in some form) may apply when the physician is asked to disclose information in court or in similar proceedings. It has nothing to do with decisions that physicians or health care facilities make about disclosing patient information in other situations.

The Federal health record confidentiality law covering the nation generally is one protecting information about patients in Federally-assisted drug and alcohol abuse treatment programs. The Privacy Act covers all Federal records, including health records, held by Federal agencies that provide health care, such as the Department of Veterans Affairs, the Indian Health Service in the Department of Health and Human Services, and the military services. For health records of the Department of Veterans Affairs, two confidentiality laws apply, including one which provides specific protections for drug and alcohol, HIV infection, and sickle cell anemia records.

All these laws permit certain limited uses of patient information without the consent of the patient where a recognized exception applies.

The array of existing laws provides some protection, but, as you know, there is no single, nationally-applicable set of legal control on health care information. We need such a standard.

Privacy in an Information-Intensive System

A health care system as diverse and comprehensive as the U.S. health care system needs careful and well-designed controls on the use of information, to minimize risks to the privacy of patients. At the same time, these controls must allow for the appropriate use of information in providing health care to the American people.

Health records are used for many purposes today—in the delivery of care to individuals, to operate the health care system, and for other purposes that are compatible with and related to the delivery of health care. People who work in a health care facility, in treating patients or in related activities like billing, need access to patient records.

Patients routinely authorize disclosure to health insurers to obtain reimbursement. Records are used for research to gain new knowledge to prevent and treat illness, often with patient identifiers so they can be linked with other records, although without further use or publication of the identifiers. Quality reviews and audits to ensure that payments and reimbursements are correct require access to records. In some instances, medical conditions are reported to public health agencies, to permit investigation and, as necessary, intervention. Health records frequently can be critical evidence in investigations and prosecutions of unscrupulous health care providers who defraud insurance programs, or deny their patients quality care.

Strong privacy protections can, if properly configured, form a backbone for the health care system. Legal controls of the type the committee is considering prevent disclosures that are not appropriate or necessary. They reassure patients that there are orderly processes for dealing with their information, even if there is not absolute secrecy. They regulate government access to and use of information about people. They ensure that patients can see their own records if they wish, and provide remedies for patients whose records have been improperly used or disclosed.

Careful protections are especially important with the widespread computerization of records. Computerization can provide great benefits both for the patients and for management of the health care system. The effect on the privacy interests of patients is mixed. Computerized records present certain new vulnerabilities, such as the possibility that an unauthorized user may get access to them through the communications system. If an unauthorized user does get access, large volumes of information can be transmitted quickly and easily, while it is comparatively difficult to transmit large volumes of information in paper records.

At the same time, computerization can enhance privacy protection many ways. For example, computerization makes it easier to identify and disclose only that information which is actually needed, rather than a patient's entire record. Likewise, information can be disclosed without identifiers at all, if identifiers are not needed; this is much simpler with computerized records than with paper records. Further, when records are computerized, a more careful watch may be kept on their disclosure, through recording and auditing mechanisms built into computerized record systems.

S. 1360 offers Federal legal protections for all health care records. We welcome this proposal, and are eager to work closely with you on it.

II. PRINCIPLES

The underlying issue in the field of medical records privacy is always how to accommodate individual control of medical information in ways which are consistent

with the overall collective intereats in (1) providing health care that is of the highest quality, that is cost effective, and that is widely available and (2) maintaining financial integrity. Although this process involves trade-offs, we believe that several steps in achieving the proper balance should be reflected in any legislation.

Empower the individual to have meaningful access to his or her own records. One of the great strengths of S. 1360 is that it would provide clear procedures available to any individual who wishes to review, copy, amend or correct his or her own records. This section of the bill is a breakthrough in privacy statutes.

Empower the individual to have meaningful control over his or her records. Today, individuals may have the opportunity to sign a consent form, but the forms are often complex and difficult to understand, uninformative, and unlimited in scope and duration. The process of consent should be taken seriously. It should genuinely inform the individual by providing notice in understandable language about the intended uses of the information. To the extent feasible, the individual should be given the opportunity to object to specific disclosures; here again, electronic technologies may facilitate greater individual control.

Provide meaningful mechanisms for redress. S. 1360 includes criminal sanctions, a civil cause of action and civil monetary penalties as remedies for violations of privacy. We support meaningful mechaniams for redress and look forward to working with the Committee on measures needed to enforce the protections of the bill.

Use emerging technologies to maximize privacy and security. S.1360 directs the Secretary to develop appropriate standards for privacy and security to be followed by health information trustees. This is a critical component of achieving the highest level of protection for such records.

Focus on the use of medical information as much as on its disclosure. S. 1360 forbids the use or disclosure of records except for purposes that are "compatible with and related to the purposes for which the information was obtained." We endorse that principle.

Adopt a national standard. We note that the bill preempts most State law. We believe that this approach is necessary to achieve the benefits of standardized, automatic claims transmission.

However, in the specialized and delicate areas of public health information, and mental health treatment information, we read the bill as providing that stronger State laws would not be preempted, so that if a disclosure is prohibited by either this bill or State law, it would not be allowed. This appears to be an appropriate exception to the general rule; however the practical application may need review.

III. ISSUES

Even with agreement on basic principles, there are several issues that are raised by S. 1360 in its present form. I will identify some of the significant ones, with our understanding that the work on refining this legislative language will continue. We look forward to working with the committee in that process.

Disclosures for treatment and payment

As introduced, S. 1360 will require a signed informed consent form to cover each diaclosure made for treatment and payment purposes. While we applaud the desire to foster individual rights that ia reflected in this provision, we believe that it needs to be adjusted to reflect the realities of multiple necessary disclosures, especially among health care personnel involved in providing care and treatment. As a practical matter, such a requirement will continue the practice of getting from patients extremely broad consent forms that will preserve the appearance of control but not its reality.

As an alternative approach, we suggest that for these two most common and necessary categories of disclosures, individuals be given the opportunity to object to the disclosure of particular information or disclosure to particular recipients of information. In other words, a physician would have the discretion to disclose to another physician, for example in the course of a consultation or referral, unless the subject had objected in advance to the disclosure of certain conditions even for purposes of securing treatment. Likewise, disclosures neccaaary to secure payment could proceed without having to secure a new consent form if, for example, a person changed insurance carriers.

Research

The bill provides for disclosure of information for research purposes in limited instances without the authorization of the individual. This accommodates the situations in which patient identifiable information is needed for research studies.

Much health research can be conducted without patient identifiers. Computerization permits ready segregation of identifiers from other information about individ-

uals, and public use files can be produced to permit extensive analysis in the many situations where it is not necessary to use identifiers to match health records with other records.

But for research where records must be matched with other records, such as death certificates, identifiable information may be needed. With appropriate safeguards, this can be done with respect for the privacy of the persons involved. The bill includes requirements to ensure that these disclosures are made only when necessary, for productive research purposes, after review by an institutional review board, with specific standards of necessity and importance. Current Federal policy and HHS regulations provide a model for such an approach. Information so disclosed should be used only for the intended purpose, and the identifiers removed as soon as possible.

Health information assembled for research and statistical purposes should be immunized from the scope of reporting laws and judicial process, as the National Center for Health Statistics now is. Health data assembled for research and statistical purposes should not be used to take any individual action affecting the rights, benefits or privileges of an identified individual. Limitation on the use of research and statistical information in this way—called the principle of functional separation—was recommended by the Privacy Protection Study Commission, in its report, Personal Privacy in an Information Society, in 1977, and the point was reiterated recently by a committee of the Committee on National Statistics in a report, Private Lives and Public Policies (1993).

Oversight and Law Enforcement

The bill as written provides for disclosure of records for the purposes of oversight. A wide variety of audit, investigative, and program evaluation activities require direct review of identifiable health records. In the vast majority of instances, the investigations are of health care providers, but there are some investigations of fraudulent actions by recipients with respect to payments for health care, and of collusion between patients and providers. These tasks are performed by the Office of Inspector General of the Department of Health and Human Services, by the Federal Bureau of Investigation, by other Federal investigative agencies, such as the Defense Criminal Investigative Service, the Offices of Inspectors General (including the Inspectors General of the Department of Labor, the Department of Veterans Affairs, the Office of Personnel Management and the Department of Defense), and by State and local agencies, including specialized Medicaid fraud units in states. We urge the Committee to work with this Department and the Department of Justice to ensure that the comprehensive framework that would be established by this legislation to address legitimate privacy concerns also address equally legitimate law enforcement concerns.

We have the following observations on the bill's provisions that permit these disclosures:

- Some investigations of fraud and abuse in the health care treatment and payment system are done by units of general law enforcement agencies, such as the Department of Justice, the Federal Bureau of Investigation, other Federal agencies such as the Drug Enforcement Administration and the U.S. Postal Inspector, and State and local police agencies. Additionally, there are civil and administrative as well as criminal enforcement agencies. Nearly every health care fraud investigation involves health records that would be covered by the bill.
- These agencies use identifiable records from health care providers in the same way as specialized health oversight agencies, and access by such agencies ought not to be made more cumbersome than is strictly necessary to preserve patient privacy interests. We note that the bill provides that if these agencies get access as health oversight agencies, they may not use patient-specific information except in actions or investigations relating to receipt of or payment for health care. This is an important protection, and is an essential corollary of the ready access that the bill allows for oversight activities.
- While the bill provides for disclosure in connection with criminal activity or to determine if a crime has been committed, it is important to recognize that many investigations seek to determine whether civil fraud is occurring.
- The bill properly provides that the information obtained in an oversight investigation may be used against the patient both when the inquiry relates to "receipt of health care or payment for health care," and when it relates to fraudulent claims relating to health. The latter is helpful in investigations of fraud in liability claims, disability program applications, and workers compensation claims.

- Patient access to their own records in the hands of health oversight agencies, and patients' awareness that their records have been disclosed by providers to investigative agencies, can, in some instances, reveal to patients that an investigation is underway, and permit evasive action. Existing individual access rights to Federal records, and in the Privacy Act, include exceptions to address these concerns.
- When compulsory legal process is used to obtain information, the bill provides, in many instances, for notice to the individual. Where the focus of the request is actually the individual, this notice may be a valuable protection. However, it should not be required if the disclosure could be made even without compulsory process under other provisions of the bill, such as disclosure for oversight purposes. It serves no purpose for the individual, could be distressing to the individual, and could impair the activities for which the bill permits disclosure. An exception should also be made for investigations involving health care payment fraud offenses. To provide notice in such cases would not be appropriate, as it would tip off suspects that they were under investigation, and would impede legitimate law enforcement efforts. For these reasons, the Administration urges modification of the bill to include a limited law enforcement exception from the notice requirements and prohibitions of the Act for health payment fraud offenses. These are typically instances in which the inquiry is focussed not on the individual, but on the provider or other record holder.

Relationship to Other Law

The relationship of the bill's requirements to other law may need to be addressed in more detail. There is no reference to the interaction of the bill with the Privacy Act of 1974, or to certain other statutes governing the activities of Federal agencies which provide health care and conduct and support health research.

In addition, with reference to research and statistical activities, it is important that the bill not eliminate more protective provisions for this information in existing law.

The Role of HHS

We have several concerns about the nature or timing of the responsibilities that S. 1360 would place on the Department of Health and Human Services.

First, the bill would require that the Secretary certify health information network services. This certification procedure is not spelled out, but could impose substantial time and resources demands on the Department. The bill would also require that the Secretary certify institutional review boards, which may include a new class of boards not now subject to Federal review, without specifying what that process would entail.

Second, the bill would require Secretarial approval of any disclosure for research to a researcher not located in an academic center, health care facility, or public health agency, even though the disclosure had been approved by an institutional review board. Direct involvement of the Department of Health and Human Services in approving individual research projects could create a cumbersome process, and could impose substantial time and resource demands on the Department. To the extent that there are concerns about certain classes of research, we are happy to work with the committee to design appropriate protections, not involving direct HHS review, for the privacy interests of individuals.

Third, the Department would be required to create a new advisory committee, subject to the Federal Advisory Committee Act, and to engage in negotiated rulemaking. We are now in the process of altering the already existing National Committee on Vital Health Statistics so that its focus would shift to issues of data standards and privacy. We believe that it would be far more efficient to use this existing committee for the purposes alluded to in S. 1360.

Lastly, the bill would require all new regulations called for by this law to be promulgated not later than six months after enactment. That is not a sufficient period of time in which to develop regulations in this very sensitive and important field.

CONCLUSION

We hope this testimony will prove helpful to the committee. In addition to the points we have made here, we have additional technical comments which we would be pleased to offer as you continue work on the bill. We stand ready to answer any questions, and to help the committee as needed.

STATEMENT OF THE AMERICAN CIVIL LIBERTIES UNION

I. OVERVIEW

The American Civil Liberties Union (ACLU) appreciates the opportunity to provide this testimony. The ACLU is a private, nonprofit organization of more than 275,000 members, dedicated to the preservation of civil liberties enshrined in the Bill of Rights and the Constitution. The ACLU has been actively involved for decades in both legislation and litigation to protect privacy rights.

Medical information is of a highly personal and sensitive nature. Medical records potentially reveal information that may render the patient vulnerable to humiliation and discrimination. The privacy interest in such information reflects an American tradition. This tradition animates doctrines such as the doctor patient privilege and the canons of the medical profession such as the Hippocratic Oath.

We thank Senator Bennett for his interest in seeking to provide privacy protection for medical records. Federal legislation is surely needed. Title I of the Medical Records Confidentiality Act of 1995, S. 1360, makes important strides in the direction of privacy protection for medical records. However, Title II of S. 1360 has some serious weaknesses that in our view would undermine the very intent of this needed legislation. Consequently, we oppose S. 1360 as introduced. However, we are confident that adequate changes can be made and we would welcome the opportunity to work with the Senate to improve Title II so that we can support this important legislation. We want to make it clear that our views should be distinguished from the views articulated by the ACLU of Massachusetts. Specifically their "Statement of Opposition to S.1360." While some of our concerns are shared by the ACLU of Massachusetts, their statement of opposition expresses objections with which we do not agree. Our statement first outlines the pressing need for legislation creating a strong federally enforceable privacy right in personal health records, and second, discusses areas of weakness that must be addressed if the Act is to achieve its laudable goal.

II. THE NEED FOR FEDERAL PROTECTION OF MEDICAL RECORDS PRIVACY

We believe that strong federal legislation which establishes enforceable privacy protection for personal health information is critical. Most Americans would be surprised to learn that what they tell their physician and what he records about their treatment are not already protected. As they learn the real situation, the awareness contributes to a growing sense of anger over loss of control over disclosure of the intimate details of their lives.

The ACLU seeks federal legislation that provides patients with meaningful control over who may have access to their records, including limiting some persons to specified information only. Re-disclosure should be prohibited except with specific permission or, in very narrow circumstances, upon express statutory authorization. We support federal privacy protection in this area for three primary reasons: first, staggering technological innovations which allow for easy transfer of personal health information over great distances; second, the expansion of managed care, which will necessarily expose confidential information to a wider network of people; and three, the unevenness of privacy protection provided by current state laws to medical records whether kept on paper-based or computerized information systems.

A. The Computerization of Health Care Data

A national information infrastructure is rapidly taking shape. Medical records, data, and images are increasingly transmitted over large distances with the push of a button. Approximately 15% of all health care records are automated and 90% of information needed to process insurance claims is automated. Current efforts at both the federal and state level will ease the increased computerization of health care information.[1] The national automation and linkup of health care data bring the lack of uniform privacy protection into high relief.

While some claim that such technological advances mean greater cost-efficiency and perhaps better health-care, such hoped for benefits must not be at the expense of privacy.

---

[1] This is manifested in Congressional health care reform bills and in the development of computerized health care information systems in states such as Iowa, Minnesota, New York, Ohio, Tennessee, Vermont, and Washington.

B. Inadequacy of Protection at the State Level

Two recent reports, one issued by the Office of Technology Assessment[2] and the other by the Institute of Medicine,[3] have concluded that federal legislation is needed because of the inadequacy of existing state laws. With the increasing "nationalization" of health care data—a trend the Act could accelerate—state-by-state protections may no longer be appropriate. Moreover, most states do not have a comprehensive statute that protects the privacy of all health information. State confidentiality laws are uneven and sometimes conflicting.

Currently, only 34 states have provided some level of privacy protection under state law. Sixteen states have enacted no legislation at all to protect the confidentiality of medical records. Of the 34 states that do have privacy laws, the privacy provisions are often found under various state statutes and enforced by different institutions, ranging from corporations to hospitals and public health authorities to insurance commissioners. Furthermore, without privacy protection at the federal level, privacy protection relies on local policies and practices. Such customs vary from place to place and typically lack effective enforcement mechanisms. The inadequacy of state laws in this area is disturbing. Without the ability to know and rely on uniform privacy protections, patients lack the basis for meaningful consent.

Therefore, especially because the Act would enable the nationalization of health care data, the ACLU strongly supports federal legislation in this area. But we do not support federal preemption of stronger state laws. S.1360 should provide a "floor" of protection, not a "ceiling." Only less rigorous state law (whether statutory or common law) should be superseded by S.1360. In the ACLU's view, state laws that now or in the future give more patient control of medical records correspond with the goal of S.1360 to protect a patient's privacy interest in his medical records. The Act should explicitly state that State rules of law that provide for greater privacy and confidentiality rights of an individual or require expanded patient access to medical records should not be preempted by S. 1360 and liability under common law must not be eradicated.

Effective federal legislation is needed to preserve the privacy interest of patients in their medical records, especially in light of increased computerization of health care data. Federal legislation, if properly crafted, has the potential to provide uniform privacy protection.

The next sections present our concerns regarding areas of weakness in S. 1360 that must be strengthened to accomplish its goal. Our comments center around the informed consent provisions; the requirements for administrative, technical and physical safeguards and access to medical records by law enforcement. It should be noted that there are other areas of concern which may be identified as we continue to analyze this proposed legislation.

III. INFORMED CONSENT

The Constitution establishes a privacy interest and an interest in bodily autonomy.[4] Both interests are offended upon disclosure of personally identifiable health information without the informed consent of the patient. For consent to be "informed," the patient must be given adequate information on which to decide. For consent to be meaningful, is must not be coerced.

The ACLU strongly recommends that the general consent requirement[5] be strengthened in two ways. First, the Act should require that medical information obtained prior to the Act without the genuine informed consent not be used unless, with carefully drawn exceptions, consent consistent with the requirements of the Act is obtained.[6] Unless this is done, the Congress will leave untouched the vast invasion of medical records privacy that has given rise to the need for this legislation while merely layering the Act's protections on the new information added to the current mountain of private data abusively obtained.

The second area in which consent should be strengthened concerns the requirement in Section 201 (b)(2) of the Act that disclosure is limited to the "minimum amount of information necessary to accomplish the purpose for which the information is disclosed." We believe that this "minimization" requirement, an important protection of the Act, already implicitly includes the requirement that the disclosure

---

[2] U.S. Congress, Office Of Technology Assessment, Protecting Privacy in Computerized Medical Information, OTA-TCT-576 (U.S. GPO, Sept. 1993).

[3] Institute of Medicine, Health Data in the Information Age: Use, Disclosure, and Privacy (National Academy Press, 1994).

[4] See Griswold v. Connecticut, 381 U.S. 479 (1965).

[5] Title II.

[6] One example of: appropriate exception might be to allow a health care provider to retain the record for purposes of resolving future questions about the adequacy of treatment.

is for the minimum period of time necessary to achieve the purpose of the disclosure, but we suggest that this should be explicitly stated in the Act.

A. Scope of Disclosures

Section 201 of the Act on scope of disclosure prohibits the use or disclosure of information unless it is "compatible with and related to the purposes for which the information is obtained." S. 1360 should require that information may be used only for the specific purpose authorized by the patient. We are concerned that this language could be used to justify disclosure and use of protected health information beyond what has been specifically authorized by the patient. The Act should explicitly limit disclosure to the specific purposes authorized by the patient.

B. Disclosure to Certified Health Information Services

Section 204 permits the "health information trustee" to reveal protected health information to a "certified health information service." Specifically, in Section 204(b) the certified health information service is granted access to personally identifiable medical records to create non-identifiable medical records. In the interest of protecting the patient's privacy interest in his medical records, Section 204(c)(1) provides that such health information services will not be "certified" until they "establish and maintain appropriate administrative, technical and physical safeguards to ensure the confidentiality . . . of protected health information."

While the ACLU supports the requirement that health information services establish safeguards for privacy, the ACLU is concerned by the lack of an informed consent requirement. Informed consent should be required from the patient before protected health information is released to a contractor of the health information trustee. This provision represents a loophole in the protections sought by this legislation. It permits a chain of disclosure without the patient's knowledge or consent. Disclosure of personally identifiable information must occur only pursuant to the informed consent of the individual. The informed consent provisions outlined in Section 203(a) should be extended to apply in the instant context. Health information trustees should not be allowed to disclose personally identifiable health information to health information services without the informed consent of the patient, and any proposed disclosure other than for payment or treatment should state the reason for the disclosure. Additionally, as part of assuring informed consent, the Act must explicitly define the manner in which patients will be informed of the process for any de-identification of "protected health information."

C. Disclosure to Next of Kin

Section 205 of the Act allows for disclosure of "protected health information regarding an individual to the individual's next of kin, to an individual representative of the individual, or to an individual with whom that individual has a significant personal relationship[7] without explicit consent. While the ACLU recognizes the importance of this provision, we have strong concerns that as written it may allow for unauthorized disclosures that may have adverse effects on a patient's ability to safeguard access to confidential medical care. We are continuing to examine this provision and we look forward to presenting this Committee with recommendations that will clarify the legislation.

D. Disclosure to Health Oversight Agency

Section 207 of the Act provides for unauthorized disclosure of "protected health information" to a "health oversight agency for an oversight function authorized by law." A health oversight agency as defined in Section 3(8) includes any number of individual representatives of agencies involved in the vast bureaucracies which monitor, license, evaluate, investigate, and certify health care providers. This wide array of Federal and State agencies are seemingly given full access to any and all protected health information that they deem necessary to their "function" as "authorized by law." This provision is unacceptably broad and may well allow for unwarranted governmental intrusions into patient's private medical records while providing no benefit to the patient. At the very least each patient must be informed that their medical records are prospectively a part of such investigation. At a minimum the Act must provide that patients be notified about proposed discloaures of these kind and given the right opportunity to veto access to records about them.[8]

---

[7] Sec. 205(a).

[8] We note that the Act makes the oversight agency a "trustee" for the agency and therefore subject to the restrictions of the Act. This is an important protection that should not be diluted by an over broad proviaion.

E. Disclosure to Health Researchers

Section 209 provides that a health information trustee may disclose protected, personally identifiable health information without the patient's consent to a health researcher if a certified Institutional Review Board (IRB) determines that the project is of sufficient importance to outweigh the intrusion into the privacy of the individual. First, it should be noted that this provision runs counter to the general approach of the Act which is to prohibit disclosure without explicit consent. Therefore, any exceptions to this general rule must be narrowly tailored to accomplish a compelling interest that cannot be accomplished by providing for the consent ordinarily contemplated by the Act.

Disclosures of personally identifiable health information without the consent of the patient could violate the patient's faith in the sanctity of his ability to control the disclosure of protected health data. While the legislation provides for IRB review, the rigor of IRB standards is highly variable throughout the country and therefore inadequate as a protection.

The ACLU urges that a separate consent form for research be required and that only information subject to such consent be available for research. At a minimum, the patient should be presented with the right to decline to have his personally identifiable records used for research purposes. Anyone who claims that the demands of medical research must override a freely exercised decision not to participate in medical research is really claiming a right both to intrude into the patient-physician relationship and to impose the researcher's values to the detriment of the patient's decision. The researchers are in effect saying they know better than the patient how valuable research is, vis-a-vis the patient's privacy interests, and have a right to convert the medical record created for treating the patient into the researchers' use over the patient's objections.

Finally, the ACLU believes that only true biomedical research conducted at qualified medical facilities and institutions should be permitted to obtain medical information under the Act, thus the definitions of health research and health researchers would need to be amended accordingly.

F. Disclosure Prohibited

With the arrival of computer-based patient records, certain zones of a patient's record can be kept completely confidential.[9] Many consumer groups and privacy advocates view the entry and electronic storage of patient-identified information into a computerized medical records "network or database" as tantamount to a disclosure, requiring explicit patient consent. We interpret the Act to already require express reference to use of such network or database either in the disclosure of information services[10] or in the disclosure forms.[11] If that interpretation is not correct, then we believe patients should have the right to give their explicit consent before their identifiable information is entered into a network or database. Even if such explicit consent is acquired, the issue remains whether the Act should allow a patient to refuse such disclosure, but still get treated or receive payment. At the very least a provision should be inserted into S.1360 that allows a patient to designate certain portions of his record as completely confidential. Upon such designation, the information contained in that zone cannot be released unless stripped of any identifier that could link it to the patient.

Such a provision would give patients another recourse by which to control information about themselves. This type of provision is in accord with the goal of S.1360 to create an enforceable privacy right in medical records.

G. Disclosure to Law Enforcement Agencies

The exceptions to the Act's general informed consent provisions which allow for access to "protected health information" by law enforcement agencies is of great concern. On the heels of much controversy regarding police abuse, we can think of nothing more chilling than the prospect of law enforcement agencies being given access to personal medical records. Any law enforcement access to personally identifiable medical records must be viewed with utmost caution. While we acknowledge that the current provision of S.1360 relating to the requirement of probable cause for law enforcement access to medical records[12] is an effort to address concerns about unauthorized disclosures to law enforcement, the approach taken is not adequately protective of personal medical information. For example, among other problems, the

---

[9] Institute of Medicine, The Computer-Based Patient Record: An Essential Technology for Health Care (Richard S. Dick, Elaine B. Steen eds., 1991).

[10] Section 103.

[11] Section 202.

[12] Section 212(a)(2).

standard for obtaining a warrant is a dilution of the traditional probable cause standard. In many ways, the issues raised here are analogous to those regarding electronic surveillance and the 'super' protection afforded tax information. Moreover, we are concerned that the "exceptions" to the need for a warrant or subpoena can lead to abuse. Apparently, under section 210(b) of the Act, an opposing attorney in a civil case, a prosecutor in a criminal case, or an administrative agency might falsely certify to a health information trustee that notice was given to an individual and allege (in good or bad faith) that the individual's mental or physical condition is an issue in a litigation or administrative proceeding and thereby obtain whatever information is sought. We will forward our recommendations for such amendments to the Committee.

IV. ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

S.1360 imposes the general requirement on health information trustees to "establish and maintain appropriate administrative, technical, and physical safeguards to ensure the confidentiality, security, accuracy, and integrity" of health information.[13] S. 1360 contains no specific technical or administrative requirements. The Act requires trustees to take "appropriate" action to "ensure" confidentiality and security. This is an extremely important part of the Act, and whether the Act ultimately serves to protect privacy will hinge in part on keeping this requirement on health care trustees undiluted.

A. Confidentiality and Security

S. 1360 should include at least some carefully drafted examples of specific safeguards to ensure confidentiality and security. Presumably, any time an unauthorized disclosure or use occurs, the trustee has failed to "ensure" confidentiality or security and so violates the Act allowing the patient to seek redress and recover damages under the Act.[14] We interpret the Act to mean that there is a violation, and therefore recovery under Section 302, any time there is an unauthorized disclosure, but this could be more explicitly stated in the Act.

Additionally, S. 1360 merely provides that the Secretary of Health and Human Services "may" use a negotiated rule making committee or an advisory committee in promulgating regulations and that the advisory committee make "recommendations for modifications in order to ensure efficient and confidential data interchange of personally identifiable information."[15] This language suggests a premium on efficiency rather than privacy. The ACLU recommends the inclusion of provisions that incorporate a minimum list of specific safeguards, for which the Secretary or an appropriate entity is explicitly required to promulgate regulations and implementing requirements.

B. Unintended Disclosures—Insider Access

The threats to privacy created by insider access to medical records is greatly increased when health care information is processed and stored on computerized health information systems. Computer and security experts state that the vast majority of violations of confidentially are due to actions of insiders. Because of mergers and increased integration of many health care providers, insurers, employers and health information management organizations, the outsiders are often brought inside.

The privacy of a patient's medical record must be maintained. This includes ensuring that only those insiders or outsiders who have an expressed need to know and the requisite patient authorization will be allowed to handle or to have access to protected health information and only for the specific purpose authorized. S. 1360's provisions on access to information by insiders must be strengthened. Supporters of the Act have stated that the Act's restrictions on disclosure already apply, for example, not only to an insurer, but to the insurer's employees. This intent, however, is not entirely clear. It is our view that such a restriction requires that a "trustee" ensure that protected health information is not accessible to its employees, contractors or agents who do not have express authority from the patient or a legitimate need to know. The Act should be clarified to emphasize the legislative intent to prohibit unauthorized disclosure of protected health information to anyone—including other employees, agents or contractors of the health information trustee.

The Act should also be clarified so that any "use" is also in effect a "disclosure" and therefore subject to the requirements of the legislation. This is already implied in the way the Act's requires specific consent for disclosure. If an employer gets in-

[13] Section 111.
[14] Section 302.
[15] Section 111(b)(1)(B)(iii).

formation for purposes of payment and "uses" that information himself (without redisclosure) for non-payment purposes, he has violated the authorization under which he got access to the information in the first place, and he would—we believe—be subject to the Act's penalties. This protection should be clarified, however.

Further protection against insider abuse would be achieved with the inclusion of a provision for "whistle blowers." Even the strongest protection against abuse by insiders is limited by the willingness of insiders to come forward with information about the abuse. S. 1360 should include both incentives for whistle blowers and protection against retaliation for whistle blowing.

V. ENFORCEMENT

S. 1360 gives the responsibility for enforcement of the Act's protections to the U.S. Public Health Services, Department of Health and Human Services (HHS). HHS, as a payer and administrator of health services, would also be subject to the requirements of this Act. The dual role of the regulator and regulated may present a conflict of interest. The responsibilities for administering this Act should be assigned either to an existing or a new administrative agency not otherwise responsible for administering or providing health care programs.

VI. CONCLUSION

While federal legislation is certainly needed, S.1360, as currently drafted, is insufficient. Unless many of the changes we recommend are adopted, the Act could have an effect opposite from that intended by Congressional privacy advocates. The ACLU is eager to work with members of this committee to achieve the peace of mind that we all seek in knowing that personal health information is indeed private and subject to our control.

PREPARED STATEMENT OF JEANNE SCHULTE SCOTT

My name is Jeanne Scott. I am Director of Government and Legal Affairs for CIS Technologies, a Tulsa, Oklahoma based health claims clearing house. CIS serves 538 hospitals and 3,000 doctors in 34 states.

I am here today as Chair of the Board of Trustees of the Association for Electronic Health Care Transactions.

I am grateful for the opportunity to testify before you and the Committee this morning.

ABOUT AFEHCT

The Association For Electronic Health Care Transactions (AFEHCT) is a trade association of venders and suppliers to the health care EDI industry. Our membership includes:

- health claims clearinghouses
- value-added networks
- software vendors
- health insurers
- managed care companies
- consulting companies
- bank companies
- health care data processing companies
- data communications systems operators

AFEHCT's members move large amounts of health care data electronically. Our member companies processed over 210,000,000 claims in 1994. That is in addition to the other electronic transactions related to eligibility, remittance advice, etc.

THE HEALTH CARE EDI INDUSTRY
WE WOULD LIKE YOU TO KNOW.....

- EDI transaction processors such as AFEHCT member clearinghouses and value added networks, for each client hospital, doctor or other provider, reduce the paper work hassle under the current multi-payer, multi-claim form environment to the simplicity and ease expected under a single payer system.

- EDI transaction processors, such as AFEHCT member claims clearinghouses and value added networks, are saving substantial amounts of money for both providers and payers.

- Because of market competition, the prices for these services are declining rapidly as the pace of technological innovation is accelerating!

- Electronic transactions can often involve several different corporate entities:

  - From the doctor's office to —

    a MEDICAL BILLING COMPANY, to a

    a VALUE-ADDED NETWORK.
    Value-added networks are companies that buy telephone time in hundreds of millions of dollar increments; and then resell that time and the management of that time to individual client health care providers,

    No value-added network has connections in all cities or with all entities so just sending a transaction via a value-added network from one point to the next point in the electronic transaction daisy chain can involve several companies and telephone companies,

    a HEALTH CLAIMS CLEARINGHOUSE, which would (1) make sure the claim was clean, that it passed all the front end edits and audits the payer would apply to the claim, and (2) reformat the claim to the electronic specifications of the payer. The health claims clearinghouse may also have a

    SUBCONTRACTOR. This would involve another set of transactions through one or more value-added networks,

    another VALUE-ADDED NETWORK involving one or more telephone companies, and

a PAYER

- The health care EDI industry deals in a very large number of financial and administrative transactions. In 1994, 3.5 billion claims were processed. Of that 1.3 billion or 36% were processed electronically. For each claim submitted, there could be as many as 11 other types of transactions such as

    - eligibility
        - inquiry
        - response
    - enrollment
    - claims submission
    - claims status
    - remittance advice
    - referrals
    - other managed care transactions

  There are also clinical transactions to consider, such as lab reports and other clinical transactions that can be sent electronically.

  Each of these transactions involves the disclosure of protected health information.

THE HEALTH CARE INDUSTRY AND PRIVACY

The EDI health care industry has an excellent record in privacy/confidentially/security of health care data.

Of all the horror stories about the abuses of privacy or confidentiality, all are anecdotal involving one person and always if not almost always in a paper environment.

The health care EDI track record is also exceptionally good when you consider the volume of health care transactions it handles (See above referenced statistics.)

WHY THIS INDUSTRY ---- WHY A NATIONAL/FEDERAL PRIVACY LAW

Although health care is delivered on a local level, it is paid for and administered on a national level. On any given electronic transaction you could have 4 to 10 or more separate corporate entities involved across as many different states. Which state's privacy law applies ? Answer: They all do.

We, as an industry, want a single set of nationwide rules to go by.

We need a single set of nationwide rules to help local markets work more effectively.

The medical record privacy issue first began to surface as a result of the Bush administration's and then the Clinton administration's interest in maximizing, as a cost saving and efficiency effort, the application of electronic data interchange(EDI) in claims processing and clinical transactions.

It was the growing impact of EDI in health care that caused privacy advocates and the EDI industry to surface the privacy issue.

S.1360, The "Medical Records Confidentiality Act of 1995"

AFEHCT has worked with Senator Bennett and his staff since the inception of his effort on behalf of S,1360. We have supported this effort with time and information.

AFEHCT believes that a national privacy law needs to be enacted.

AFEHCT believes the privacy/confidentiality/security of a patients medical information is a positive social good. We also believe the promise of EDI in health care is a positive social good in that it will among other things

- Move health care data much faster and much cheaper,
- Make individually identifiable health care data much more secure.
- Make it easier and more cost effective to assemble data for the kinds of analysis that would support market based principles in the delivery of health care.

in this bill, these two positive social goods are in tension with one another.

However, S.1360, as introduced, maximizes the privacy/confidentiality/security protections for patients and individuals, and does great harm to the health information service industry.

To **optimize** the privacy/confidentiality/security protections for patients and individuals, and to optimize the promise of the health care EDI industry S.1360 needs to be modified as follows:

- The authorization for disclosure of protected health information to health information services must be restored.
- The need for a "very bright line" distinction between the duties and obligations of a health information service when it is acting as an "agent" or "contractor" to a provider/payer trustee and when it is acting as a trustee must be addressed
- Language should be included that creates a neutral to positve market environment for the health information services industry/the health care EDI industry by allowing

companies if they wish and within the bounds of contracts with health information trustees they serve

- to retain protected health information, and
- to use it, but not disclose it, in research that woud support services that could improve the cost effectiveness and efficacy of the delivery of health care.

We believe Senator Bennett's bill, S. 1360, could be an excellent vehicle for arriving at a bill and ultimately a statute that optimizes the privacy/confidentiality/security for patients and individuals in concert with preserving the promise of electronic data interchange in health care.

However AFEHCT and its members have a number of serious concerns about the bill. These include:

- Health Information Services such as health claims clearinghouses and value added-networks are wiped out.
- The definition of a Health Information Trustee and the confusion arising therefrom
- Time Frames for Implementation
- Preemption of State Law
- No Liability for Permissible Disclosures
- Establishment of Safeguards
- Inspection and Copying of Protected Health Information
- Correction or Amendment of Protected Health Information
- Accounting for Disclosures
- Authorization for Disclosure.

HEALTH INFORMATION SERVICES WIPED OUT

As introduced, this bill would wipe out the entire health information service industry.

Under Section 201(a) GENERAL RULE a health information trustee may not disclose protected health information except as authorized under this title.

In earlier drafts of the bill, section 204(a) contained an authorization for "a health information trustee to disclose protected health information to a health information service acting as an agent or contractor.

This provision was later deleted from the bill for reasons not entirely clear.. Without this authorization trustees may not disclose protected health

information to health information services; and health information services are effectively wiped out.

This authorization must be restored. With out this authorization AFEHCT make every effort to defeat the bill.

HEALTH INFORMATION TRUSTEE CONFUSION ARISING OUT OF THE DEFINITION

According to the definition of a health information trustee contained in section 3(7), a health information service is included as a health information trustee by specific reference in subsection (A) and indirectly in subsection (C) as an "agent or contractor" to a trustee.

Accordingly any one who comes into contact with individually identifiable heath information -- protected health information -- is automatically a health information trustee.

If a health information service is always a trustee and has to assume the duties and responsibilities of a trustee under the Act then the system breaks down.

Let me give you just one example. It has to do with Authorizations

In order to disclose protected health information (and all health care claims and related transactions e.g. eligibility transactions, claims status transactions, remittance advices, etc. are all protected health information) a hospital, doctor or other provider of health services, as a trustee, must obtain an authorization.

In the electronic claims process/submission, the claim may have to pass through several different corporate entities:

- a value added network to the
- health claims clearing house to another
- value-added network.

Because no one value added network has connection in all cities or locations, several value added networks may be involved in getting the electronic claim from party A to party B.

Similarly claims clearinghouses may subcontract out some of their functions.

If, in order to disclose the claim to the next corporate entity a written authorization to disclose must be obtained from the patient, then a transaction that could take seconds could take days, weeks, or even months. A transaction that costs pennies, could end up costing several dollars.

That is not beneficial to the consumer, the provider, the payer or any one involved.

What is needed here is legislative language that is more reflective of how business is being conducted today. Providers and payers need to be able to contract with agents and contractors to fulfill their obligations under this Act.

Health information services, agents, and contractors need to be able to contract with providers and payers without having to assume, in duplicate, all the obligations of a trustee.

In an ideal setting, health information systems, as a agents and contractors would negotiate the fulfillment of these duties (see list below) between them.

Section	Title	Trustee	Trustee's Agent
101	Inspection and Copying of Records	Required	Negotiated between Trustee and Agent
102	Correction or Amendment of Protected Health Info.	Required	Negotiated between Trustee and Agent
111	Establishment of Safeguards	Required	Negotiated between Trustee and Agent
112	Accounting for Disclosures	Required	?
	Maintain Record of Disclosures	Required	Negotiated between Agent and Trustee
201	General Rules Re: Use and Disclosure	Required	Required
202	Authorizations For Disclosure of PHI Treatment/ Payment	Required	Not Required
203	Authorization for Other Than Treatment or Payment	Required	Required

Recommended Solution:

The legislation should be reworked so that there is a "very bright line" distinction between the duties and obligations of a health information service when it is acting as an "agent" or "contractor" to a provider/payer trustee and when it is acting as a trustee.

Failing that health information services and agents and contractors to a trustee should be removed from the definition of a trustee.

We are working with staff and others to resolve this issue. If we are able to resolve this issue a number of AFEHCT's other problems with this bill go away.

TIME FRAMES FOR IMPLEMENTATION

Section 403 EFFECTIVE DATE requires the Secretary to promulgate regulations implementing this Act not later than 6 months after the date of enactment of this Act. It also requires that the ACT take effect 12 months after the date of enactment.

These time frames are much too short. The regulations implementing this Act will deal with some very complex issues. It will take several months develop proposed regulations . The private sector ought to be given 90 to 120 days to respond. After the response period, it will take several months to write and publish the final regulation.

The effective date of 12 months after the date of enactment is too short for the health care EDI industry to gear up.

PREEMPTION OF STATE LAW

Section 401 RELATIONSHIP TO OTHER LAWS, with a small number of specific exceptions preempts State law in the area of privacy. A strong State preemption is absolutely essential for furthering the promise of EDI in health care. AFEHCT would hope that this section would remain intact as is.

NO LIABILITY FOR PERMISSIBLE DISCLOSURES

Section 402 NO LIABILITY FOR PERMISSIBLE DISCLOSURES. Under this section a health information trustee who makes a disclosure of protected health information about an individual that is permitted under this title shall not be liable to the individual for such disclosure under common law.

This provision is absolutely essential for AFEHCT members.

ESTABLISHMENT OF SAFEGUARDS

Section 111 of the bill grants the Secretary broad authority to promulgate regulations governing the administrative, technical and safeguards to be used by health information trustees to ensure the confidentiality, security, accuracy, and integrity, of protected health information.

AFEHCT members are uniformly troubled by the broadness of the grant of authority to the Secretary in this section. One member observed

> "This broad authority is troubling because the potential for expensive and possibly unnecessary requirements exists. Security needs to be regarded as a technical issue rather than a policy issue. While policies are specifically defined, technical issues allow the creativity necessary in a changing industry. This section should address the ends (personal privacy protection)

rather than the means and allow health information services to demonstrate reasonable compliance. ..."

Paragraph (B) of subsection (b) provides under certain conditions for the appointment of an advisory group of knowledgeable individuals. The advisory group shall consist of 7 to 12 individuals including representatives of

- health care professionals and health care entities
- health care consumers
- third party payers/administrators
- privacy advocates.

The advisory group

- reviews proposed regulations and comments to the Secretary,
- assists Secretary in establishing standards for compliance with the rules and regulations.
- assists the Secretary in developing an annual report to Congress

The Secretary may promulgate regulations in consultation with privacy, industry, and consumer groups.

AFEHCT supports the concept of an advisory group. However the advisory group should be extended to include the following categories of members:

health claims clearing houses
value added networks
health data processors

We believe the legislative language should be amended to allocate membership on the advisory group as follows

Membership Category	Number of Members 7	12	25
Health care professionals health care entities	1	3	6
Health care consumers	1	1	3
Payers / Administrators	1	3	6
Privacy advocates	1	2	4
Health claims clearinghouses	1	1	2
Value added networks	1	1	2
Health data processors	1	1	2

AFEHCT believes that as a minimum, the advisory group have 12 members.

The below listed problems go away if we can successfully resolve our problems associated with the drawing a brighter line distinction between the duties and obligations of a health information service when it is acting as an "agent" or "contractor" to a provider/payer trustee and when it is acting as a trustee.

Failing that health information services and agents and contractors to a trustee should be removed from the definition of a trustee.

INSPECTION AND COPYING OF PROTECTED HEALTH INFORMATION

As the bill is written, the burden of an individuals right to inspect and or copy his or her protected health information falls upon the health information trustee.

This section requires health information trustees (providers, payers and health information services) to make available upon request

Except as provided, a health information trustee (a health plan, provider, or health information service) shall permit an individual who is the subject of protected health information or the individual's designee, to inspect and copy protected health information concerning the individual...

A health information trustee may recover the costs of inspection and copying from the requester.

Exceptions are limited.

There is a 30 day deadline within which the trustee has to comply or deny the request for inspection or copying.

AFEHCT members believe that the first line of responsibility for inspection and copying of protected health information should rest with the provider or the payer.

The inspection and copying obligations that an agent or contractor of the trustee/provider/payer should be the subject of contractual arrangements between the trustee payer and/or provider and its agent or contractor.

Senators should be aware that many health information services only retain information for as long as it is necessary to back up the transaction, about 90 days or so. If they keep information it will be sorted by provider, plan or the party with whom they have the contract. Elsewhere in the bill a trustee including a health information service would be required to retain records of disclosures for 10 years. To search for a person's information over a 10 year period can be very, very costly -- hundreds if not a thousand dollars or more.

AFEHCT believes the legislative language ought to be amended so that it is clear that where a health information service is serving as an agent or contractor to a trustee the inspection and copying function is a shared responsibility depending upon who does what to be negotiated between the two parties.

CORRECTION OR AMENDMENT OF PROTECTED HEALTH INFORMATION

AFEHCT members strongly believe that the burden of correcting or amending protecting health information, particularly claims data, should rest with the provider.

If it is desirable to preserve the accuracy or integrity of the data, then it is essential that the provider/physician approve and attest to the accuracy of the correction the individual/patient might want to make. The accuracy and integrity of the data is of the utmost Importance because the data reflect not only on the patient but also on the hospital, doctor, and each entity involved in the claim.

ACCOUNTING FOR DISCLOSURES

The first and foremost question we need to ask is a health information service in this situation a trustee or is it an agent or contractor to the trustee. the implication of that decision are tremendous. For one thing, if a health information service is always a trustee that will mean the number of data bases of protected health information will be multiplied way beyond geometrically. This can only increase the chances for violations of privacy.

Every transaction that a health claims clearinghouse, value-added network, health data processor conducts involves protected health information. Every eligibility transaction (both to and from the payer), every claims submission, every claims status report, every remittance advice involves protected health information.

There was near unanimous objection that a record of disclosure be kept for 10 years. This was viewed as too costly. Value-added networks, who for the most part are the connectivity between parties, do not look at the content of the transaction as it's going through. They definitely do not keep a record of the content of the transaction.

As a matter of fact and/or practice value-added networks do not uniformly keep records of individual telephone calls from party A to Party B This would result in accounting for millions of 10 second calls. it is unnecessarily costly.

This is also likely to be true for 800 #s.

Health claims clearinghouses, value-added networks, health data processors disclose protected health information under the terms of a contract, at the direction of the provider or payer.

The legislation ought to be rewritten or amended so that the initial burden for accounting for disclosures rests with providers and payers; and that it be

recognized that payers and providers are able to fulfill their obligations under the Act through their agents and contractors.

AUTHORIZATION FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION

Electronic data interchange(EDI) in administrative and financial transactions only works if health care claims clearinghouses, value-added networks, health data processors are considered agents or contractors of the trustee; and the burden of obtaining the authorization for disclosures rests with the provider or payer.

The burden of obtaining the authorization should rest with the provider or the payer.

Madam Chairman, members of the committee, I and AFEHCT, again wish to express our gratitude for the opportunity to appear before you today. We look forward to working with the Committee, Senator Bennett and the cosponsors of this legislation toward improving this legislation so that it optimizes the privacy/confidentiality/security for patients and individuals in concert with preserving and promoting the promise of electronic data interchange in health care.

ANNUAL PERCENTAGE OF ALL HEALTH CLAIMS PROCESSED ELECTRONICALLY
(IN MILLIONS)

Year	Total	Manually	Electronically	
			#	%
1984	2,090	1,989	105	5%
1985	2,180	2,049	131	6%
1986	2,280	2,131	148	6.5%
1987	2,390	2,223	167	7%
1988	2,470	2,272	198	8%
1989	2,590	2,182	408	16%
1990	2,730	2,212	517	19%
1991	2,920	2,319	654	22%
1992	3,130	2,319	811	26%
1993	3,340	2,261	1,079	32%
1994	3,480	2,209	1,271	36%

Source: Faulkner & Gray's Automated Medical Payments Directory, 1995 Edition

PERCENTAGE OF CLAIMS PROCESSED ELECTRONICALLY
BY TYPE OF PROVIDER
IN 1994
(IN MILLIONS)

Provider Type	Total	Manually	Electronically	
	#	#	#	%
Hospital	373	75	298	80%
Physician	1,950	1,599	351	18%
Pharmacy	725	145	580	80%
Dental	410	373	37	9%

Source: Faulkner & Gray's Automated Medical Payments Directory, 1995 Edition

PREPARED STATEMENT OF AIMEE BERENSON

The Need For A Comprehensive Federal Medical Records Privacy Law

Good morning. My name is Aimee Berenson, and I am Legislative Counsel for AIDS Action Council, the Washington representative of over 1000 community organizations across the nation serving people with HIV/AIDS. I want to take this opportunity to thank the members of this Committee, especially Senator Kassebaum, for the strong leadership you have provided in bringing the critical issue of protecting the privacy of medical records to the forefront, and for giving AIDS Action the opportunity to testify here today about the importance of this issue for people living with HIV/AIDS across this nation.

Protecting the confidentiality of health information is not merely an academic concern for people living with HIV/AIDS. Tragically, the over 1.5 million Americans currently infected with HIV not only face a battle against the disease itself, but against the fear, prejudice, stigma and discrimination that have been the darkest companions of this AIDS epidemic. People living with HIV/AIDS have lost their jobs, their homes, and the companionship and support of their families, friends, co-workers, and communities as a result of their illness. Perhaps even more appalling is the fact that people living with this disease have found themselves discriminated against in the health care system itself -- by doctors, dentists and hospitals who refused to treat them, or by insurers who denied their claims or capped their benefits.

Studies have shown that just the fear of breach of confidentiality may deter people from being tested for HIV, and that people who suspect that they may be HIV-positive delay early detection and treatment to avoid the potential negative consequences which flow from confidentiality breaches.[1] Thus the lack of confidentiality protections may cause people to avoid early detection and treatment of their HIV disease, treatment which can greatly improve both the quality and duration of life. Others are frightened into obtaining medical care and services under assumed names or obtaining only that care which they can afford out-of-pocket, in order to protect themselves, their families, and their friends.

The lack of any federal medical records privacy law has meant that people living with HIV/AIDS and their advocates have been forced to fight the battle to protect the confidentiality of their health information state by state, government agency by government agency, and case by case, struggling to make a patchwork of state laws that all too often provided little or no protections work. At the same time, we battle attempts to further stigmatize and discriminate against people with this disease by mandating disclosures of highly personal health information for political rather than public health purposes.

In some states, efforts to carve out strong HIV confidentiality protections have been fairly successful -- Massachusetts, New York and California are notable examples. In other states, such as Illinois, for example, people living with HIV/AIDS have faced the chilling specter of highly politicized attempts to access legally protected information (namely information provided for public health surveillance purposes) in order to conduct witch hunts to ferret out HIV-

[1] American Bar Association AIDS Coordinating Committee, Issues Relating to AIDS and Health Care Reform, at 30-31 (July 1993).

infected individuals.

The confidentiality of personal health information generally is not well protected today. Currently, only thirty-four states have any level of privacy protection under state law. Fourteen states have enacted no legislation whatsoever to protect individual privacy interests. Of the thirty-four states that do have privacy laws, the privacy provisions are often found under various state statutes and enforced by different institutions, ranging from corporations to hospitals and public health authorities to insurance commissioners. The legal standard governing the collection and use of health information may depend on the type of information collected (e.g., HIV status, record of abortion or record of general physical exam), the individual or institution collecting it (e.g., a federal entity, a federally funded entity, a state entity or a private entity), and whether the information is required by a third party for purposes of payment. Furthermore, in the absence of any comprehensive privacy law, the degree of protection for personal health data depends on the local policies and practices governing those who handle health information. Individuals who view such information may be bound by employer policy or ethical codes to respect the privacy of the individual to whom the information pertains. However, no consistent policy or code exists, and existing policies often lack enforcement mechanisms.

Protecting HIV-related health information has been complicated by the fact that in many instances, health care information generally is not protected. In other words, in many instances only certain pieces of health information are protected -- for example, the fact that an individual has been tested for HIV -- while all other information about the individual, for example that the individual is getting a prescription filled for AZT -- is not. And in some instances, information is protected only in the hospital or health care provider setting, so that even information that may have been protected at some point is no longer protected once it is sent to an insurance company or social service provider. Thus, even in states that have HIV-related confidentiality protections, the extent of those protections may be limited.[2] Computerization, needless to say, adds to the potential universe of people and entities who may have access to information, and further heightens the already-existing fears people have about potential breaches of confidentiality.

In developing state laws to protect the confidentiality of HIV-related information, AIDS advocates have focused on two areas: limiting the uses and disclosures of HIV-related information, and ensuring that individuals have control over (and thus confidence in) how personal health information may be used. Unfortunately, what we have found to often is that the traditional "informed consent" model of protecting health care information does not work well, because individuals may not realize the actual universe of people and entities that have

---

[2] For example, a California Court of Appeal, while sustaining the plaintiff's state constitutional privacy claim, held that the state's HIV confidentiality law only applies to disclosure of the actual record of an HIV blood test result, and not to disclosures of information obtained from other sources regarding an individual's HIV status. Estate of Urbaniak v. Newton, 226 Cal.App.3d 1128, 277 Cal.Rptr. 354, 362 (Cal. App. 1991).

access to their personal health information, or understand that there are few limits on the uses or disclosures of information that those with access may make.

For example, many states have laws requiring written consent for HIV-antibody testing, and in the course of executing that consent, people are usually made aware that, depending on state or local public health laws, their HIV/AIDS status may be reported to public health departments for public health purposes. Yet like most Americans, people living with HIV/AIDS are much less likely to realize that within the physician's office, hospital, laboratory, or pharmacy, their medical records may be accessed -- and potentially disclosed -- by anyone from nurses and technicians to orderlies and receptionists to billing departments.

Moreover, individuals are routinely required to sign forms authorizing the health care provider to disclose information to insurers, without being told that this authorization gives the insurer access to their entire medical record. Moreover, even if people were told this, most are not in a position to do anything about it. A refusal to sign the authorization means the provider cannot be reimbursed, and thus is unlikely to provide treatment or services unless the individual has the ability to pay the costs out-of-pocket, and usually on the spot. Again, the insurers' access means that many people, from claims processors to utilization reviewers to accounting department personnel, have access to the individual's medical record. Even employers may get information from that medical record, if for example the employer is self-insured, or if a third-party insurer decides to provide that information to justify premium hikes based on utilization costs, pre-existing conditions, etc.

This poses a devastating dilemma for people living with HIV/AIDS, who are forced to disclose their illness in order to get insurance companies and medical professionals to provide care, yet may in fact find themselves denied that care, legally or otherwise, on the basis of the very information they must disclose to get care.

In essence, although people with HIV/AIDS continue the decade-long struggle to create confidentiality protections out of a hodge-podge of constitutional, state, regulatory, and common-law provisions, we still face a situation where the holes are too big, the ground beneath us too unstable, and the costs too great to continue to fight this fight as we have been. It is time to address the failure of our health care system to respect and protect the dignity and privacy of those it is supposed to serve.

The Medical Records Confidentiality Act

We believe that without strong, comprehensive federal legislation, personally identifiable health information will continue to be left unprotected, and the incidence of misuse and inappropriate disclosure of such information will only increase.

When federal health information privacy bills were introduced last year, we developed criteria that we believed were essential to ensuring that such a law is both meaningful and effective. Such a law must:

- Provide a strong, uniform "floor" of protection for all personally identifiable health information.
- Place a legal duty on all individuals and entities which create, collect, or use personally identifiable health information to protect the confidentiality of that information.
- Clearly define permissible uses and disclosures of information and build "firewalls" to prevent the use or disclosure of information for unauthorized or incompatible purposes.
- Provide individuals with sufficient notice and opportunity to limit access, use and disclosure of personally identifiable health information.
- Provide strong, effective legal remedies and sanctions for violations of the law.

While there are several provisions in S. 1360 that need to be improved, particularly those dealing with health research, oversight, and administrative warrant standards and procedures, we feel that overall the Bennett-Leahy bill is a good bill that comes closer than any other to meeting these key criteria, for the reasons outlined below.

Providing a strong, uniform "floor" of protection for all personally identifiable health information

The truth is that most states do not have a comprehensive statute that protects the confidentiality of all health information in an individual's medical record, and that the provisions of the Bennett bill are more comprehensive and rigorous, the penalties stiffer, and the enforcement mechanisms more comprehensive than just about any existing privacy law protecting health information at the state level.

However, the issue of providing a floor, as opposed to a ceiling, of protections is critical because over the course of the AIDS epidemic, enormous effort has gone into creating at least some state public health laws that do provide protection for people and thus give them the confidence to come forward to be tested and treated for HIV. It is essential that we not undermine the progress, however limited it may be, that we have made in the last 12 years of this epidemic.

In fact, the very existence of the AIDS epidemic demonstrates the wisdom of setting a strong floor of federal protections, rather than a ceiling. If this hearing had been held in 1979, none of us would have foreseen the devastating epidemic that is now upon us, or understood in quite so profound a manner, perhaps, how the lack of strong, uniform privacy protections for medical records would affect so many Americans in so many ways as it has in the course of this epidemic. No matter how strong and comprehensive the law we create today may be, we must not preclude states from taking action in the future to provide greater confidentiality protections if necessary. In the 12 years of this epidemic alone, no federal medical records privacy law has been enacted. We cannot risk that some state needing to provide greater protections than we develop in this law in order to protect its citizens in some future situation will be forced to wait for Congress to act.

Having said that, we believe that S. 1360 meets the goal of providing a strong floor of

protections while explicitly exempting from preemption any state law relating to public or mental health which provides greater protections for health information than the federal law provides.[3] S. 1360 creates a strong, comprehensive confidentiality law while explicitly protecting:

** any State law relating to public or mental health that prevents or restricts disclosure of protected health information otherwise allowed under the bill;
** any Federal law or regulation governing confidentiality of alcohol and drug individual records; or,
** the Americans with Disabilities Act of 1990.

Thus to the extent such laws do in fact provide additional protections or requirements, they will remain in effect to govern the treatment of particularly sensitive mental health, HIV, STD, alcohol, and drug records. This protection is a major reason why the bill has the support of consumer-oriented groups like AIDS Action Council; without such a provision, we would not support the bill.

Placing a legal duty on all individuals and entities which create, collect, or use personally identifiable health information to protect the confidentiality of that information

In order to be meaningful, a federal medical records confidentiality law must protect all personally identifiable health information, regardless of who is collecting or using the information. As I stated earlier, the situation today is such that personally identifiable health information about one's HIV status may be protected in the context of the doctor-patient relationship, for example, but the exact same information, once provided to an insurer so that the patient can pay to see that doctor, may not be protected.

In fact, health care providers today routinely disclose health information to health care corporations which, in turn, subcontract with others to process that information, all without patient knowledge or consent. This is currently a common practice in the health care system in this country, and there is no law that regulates this practice now, which is why federal legislation is so desperately needed.

S. 1360 begins to address this problem by creating significant, comprehensive protections that do not otherwise exist today. First, the bill establishes a comprehensive definition of what constitutes protected health information, so that not only is an individual's HIV test result protected, for example, but all information about that individual's past, present or future health care, condition and treatment is protected.[4] Second, S. 1360 sets out a comprehensive definition of "health information trustees" imposing a legal obligation to maintain the confidentiality of such information on all those who collect, use and maintain health information about an

---

[3] Section 401 (c)(3).

[4] See Section 3(14).

individual.[3]

These protections are enormously important. It is estimated that during a person's single encounter with the medical system, approximately 80 individuals view health information about that person. Most states do not have a comprehensive statute that protects the confidentiality of that information, and thus the degree of protection for personal health data depends on the local policies and practices governing those who handle health information. The 80 individuals who view an individual's health information may be bound by employer policy or ethical code to respect the privacy of the individual to whom the information pertains; or they may not be bound at all. Worse still, even where such policies exist, they almost always lack and real enforcement mechanisms.

The Bennett-Leahy bill places a legal obligation to protect the confidentiality of personally identifiable health information on every single one of those 80 individuals. Whether you are the person who reviews claims, the auditor, or the provider, under this bill you are legally obligated to respect patient privacy and abide by the rules or you will face legal penalties.

The bill imposes the same obligation to respect patient privacy on every entity that touches the information.

We do not believe, as some have suggested, that this bill creates a special statutory framework to develop large information megabusinesses. Megabusinesses don't need a federal law to help develop the information superhighway -- they've already created it. While the bill does not prohibit health information from being computerized, it certainly does not assist in the development of large information megabusinesses.

Instead, one of the reasons we believe this bill is so important is that it addresses reality. Automation is here and expanding. The companies involved in the information industry have been, and will continue, to enter the health information field, with or without legislation. Today, over 90% of all the information needed just to process insurance claims moves electronically, including information about an individual's diagnoses and treatment.

We must move to provide the strong, comprehensive protections for individual medical records which do not exist today. This bill neither creates nor prohibits computerization, but it does regulate a system that we believe is dangerously out of the control of individual health care consumers. This bill will prohibit the information systems with whom health care providers contract -- to complete billing and claims transactions for example -- from capturing and using personal medical records information for any other purpose without the consent of the patient.

---

[3] See Section 3 (7).

Clearly limiting the permissible uses and disclosures of information and creating "firewalls" to ensure that information collected and used for specific purposes cannot be used for other, incompatible purposes

Obviously, ensuring that the universe of people and entities that currently have access to medical records information are legally obligated to protect the confidentiality of personally identifiable health information is critical. Equally critical, however, is ensuring that the uses and disclosures of such information are clearly defined and appropriately limited.

S. 1360 establishes explicit, comprehensive, uniform federal rules defining and limiting uses and disclosures of personally identifiable health information. Health care trustees cannot disclose protected health information about an individual without that person's authorization except in specifically-defined statutory situations. In reality, these statutorily-defined exceptions do not necessarily create access where there is no access today; instead, these statutory "exceptions" to the written authorization requirement close what is now a virtually unbounded universe of situations where your medical records can be used and disclosed without your knowledge or consent.

Moreover, the bill restricts all use and disclosure of information to the "minimum amount ... necessary to accomplish the purpose of the disclosure."[6] This "minimization" rule means that information attained for one purpose, by a doctor, insurer or health plan, cannot be used for another purpose without consent of the individual. For example, if a doctor, insurer, "health care corporation" or anyone else wants to use personally identifiable information to do cost-containment analyses, they must obtain patient consent for this use of information, on a form that is separate from the form that authorizes the information to be used and disclosed for treatment and payment. Moreover, the bill's "minimization" rules mean that if an individual files a workers compensation claim with their employer for a lower back injury, for example, any disclosure made to adjudicate this claim would be limited to the information necessary. The goal of the "minimization" rules is to eliminate disclosures of material that are not related to the claim at issue – in this example, records about the injury could be released, but not records relating to other treatment.

One of the statutory exceptions that especially affects people living with HIV/AIDS involves "public health" activities. The bill does two important things in this regard. First, it separates legally-authorized public health uses and disclosures of information from other types of health information uses and disclosures. This is essential because much concern has centered on the fear that HIV-related health information collected for public health purposes could be accessed, disclosed, or misused if there are insufficiently strong "firewalls" between public health information collection and uses and other data collection and uses. Second, by maintaining a "firewall" between legally-authorized public health reporting and all other types of health information uses and disclosures, the bill protects both the integrity and autonomy of

---

[6] See Section 201 (b)(1),(2).

state and local public health systems.

We do have concerns about particular aspects of at least three other statutory exceptions to the written authorization requirement, however: the health research exception, the oversight exception and the administrative warrant/procedures exception. These are discussed in greater detail later in my testimony.

Providing individuals with sufficient notice and opportunity to limit access, use and disclosure of personally identifiable health information

The bill clearly asserts that individuals should be able to control the flow of their medical records. Under the bill, an individual's consent must be attained prior to releasing information to any one -- even those with a legitimate "need-to-know" -- in all but a few clearly spelled out circumstances. And this bill gives individuals the right to inspect -- and correct -- their own medical records, a right which is an essential prerequisite to informed decision-making about access, use and disclosure of information.

Unfortunately, many people believe -- erroneously -- that these simple protections exist today. They do not. Even the United States Supreme Court has not found a generalized right to "control access to personal information" held by third-parties. Where individuals do have a right to control and limit the use and access to personal medical records, that right has been established by state statute. Yet in 28 states in this country an individual does not have a legal right to access her own records, even though everyone from doctors to insurance agents to billing companies and pharmacists may have such access.

And the current state of the law today is such that all too often, particularly sensitive information such as psychiatric or psychological treatment, or one's HIV status or treatment, is as accessible in a patient's medical record as the patient's height and hair color.

In contrast, the Bennett-Leahy bill puts control over the accessibility of information squarely with the patient, who must give authorization for disclosures. In addition, even when a patient authorizes disclosure, the trustee is still obligated to disclose the minimum amount of information necessary to meet the purpose of the disclosure.

Providing strong legal remedies for violations

A law may provide the most comprehensive privacy protections imaginable, but unless there are strong and effective mechanisms to enforce those protections, the law is meaningless. Since the beginning of the AIDS epidemic, the struggle to fight the disease has been complicated by attempts to fight people with HIV/AIDS. Too often, the policies and practices of governments and institutions have stigmatized people with HIV/AIDS and condoned, implicitly or explicitly, the denial not only of essentials like jobs, housing, health care and insurance coverage, but of fundamental rights to privacy, dignity, and equality as Americans.

The creation of a federal medical records confidentiality law presents the promise of a fundamental change in one aspect of the lives of people infected with and affected by HIV. This promise, however, can only be realized if strong, effective, and accessible enforcement mechanisms are available to deal with those who violate the law.

Therefore, we believe that any federal medical records privacy law must create a private right of action to redress violations. Moreover, the penalties for such violations must be significant enough to serve as a true deterrent, particularly in light of the financial incentives that may exist to violate an individual's right to privacy and confidentiality. There must be civil penalties for those individuals or entities that fail to comply with the provisions of the law, to vindicate the strong public interest in protecting medical records. And given what may be substantial financial incentives to violate the law, there must be criminal penalties for those who knowingly violate the law for profit or monetary gain.

S. 1360 provides these important enforcement mechanisms, and thus we believe the bill tries to ensure that the law provides more than just paper protections.[7] The bill provides for both civil and criminal penalties for violations of the law. Moreover, frequent violations which constitute a business practice are not only subject to a penalty of up to $250,000, but will result in exclusion from participation in Medicare and/or Medicaid -- a potentially significant deterrent in our opinion.

Recommended Modifications to S. 1360

We believe that S. 1360 provides a strong framework for a meaningful and effective federal medical records confidentiality law. However, there are several provisions in the bill which we believe should be clarified or corrected. Among the most important of these are the following:

Health Research. We do not believe there should be a broad or routine exception for health research activities involving personally identifiable information. Oftentimes research can be conducted using anonymous aggregate data. Moreover, where personally identifiable data is in fact necessary for the effectiveness of a research project, it is almost always possible to get an individual's consent prospectively.

Moreover, we are concerned that the type of research which is conducted using medical records information is not sufficiently limited in the bill. We believe that only true biomedical research conducted at qualified medical facilities and institutions should be accorded special consideration in this bill, and believe that the definitions of health research and health researcher must be amended accordingly.

To the extent such research requires personally-identifiable medical information,

---

[7] See Title III.

exceptions to consent must be narrowly-tailored. Current federal regulations governing NIH-funded biomedical research offer a model for conducting such research, and we would urge amending S. 1360 accordingly. These regulations presume that consent will be obtained, and that presumption may only be overcome upon the finding of an Institutional Review Board (IRB) that such records are required for the effectiveness of the research; obtaining consent is not feasible; and the significance of the research outweighs the intrusion into patient privacy.

Oversight Activities. The bill permits access to personally identifiable information for a specific category of oversight activities, such as oversight conducted in administering Medicaid and Medicare programs. We believe the definition of oversight activities must be clarified and narrowed to ensure that only appropriate activities and entities are covered by this exception. We note, however, that under the provisions in this bill, information accessed may not be used to prosecute the individual unless the action or investigation arises out of and is directly related to the receipt of health care or payment for health care or a fraudulent health care claim, and support this important provision.

Administrative Warrants. We believe the bill should incorporate more than a "probable cause" standard, and would urge that the bill be amended to require "clear and convincing evidence that the information is relevant to a legitimate law enforcement inquiry being conducted by the government authority". We understand there is precedent for using such a standard, and that, when combined with the "minimization" rules, such a change will place appropriate limits and safeguards on law enforcement access to information.

Civil Litigation. We are concerned that the bill does not set out clear procedures for objecting to the release of medical records in civil litigation. Currently the bill allows such access if the party seeking the information certifies that the subject of that information has put their health status at issue in pending litigation. The bill requires a 10 day waiting period after notification to the individual before disclosure is allowed, ostensibly to provide a time period for objection. However, the actual procedure for lodging objections and prohibiting disclosure is not spelled out, as it should be, under the bill, and we urge that it be amended to do so.

Conclusion

The enactment of a comprehensive federal law that protects the privacy of medical records is critical, to people living with HIV/AIDS and all Americans. People living with HIV/AIDS, perhaps more than any other group of Americans, have suffered the real consequences of the lack of such protections. Many people with AIDS have lost their lives because of this disease; but many have lost their jobs, their homes, their insurance coverage, their privacy -- not because of disease, but because of fear, hate, prejudice, and discrimination.

Congress has the power -- and the moral imperative -- to enact strong, comprehensive federal legislation to protect the privacy of medical records. Such legislation will move us that much closer toward ending the intolerable epidemic of discrimination that has tragically accompanied the AIDS epidemic in this country.

STATEMENT OF WAYNE R. TRACY

Re: Comments on the Bennett Bill S.1360 as introduced - 4th Draft

A. *INTRODUCTION*

This document represents my critique of the aforementioned bill. I believe my twenty three years as a worker in medical informatics since completing graduate school under an NIH fellowship qualify me to opine on the subject. For the last seventeen years I have served on various healthcare informatics standards committees including ANSI HISPP, ASTM E31, IEEE MIB (P1073), IEEE Medix (P1157), and HL7. Prior to graduate school, I delivered direct patient care as a US Navy corpsman and as a medical technologist and lab manager in civilian life. I have also commanded a US Naval Reserve field hospital unit. During my career I have held direct managerial and technical responsibility for the development and deployment of numerous clinical information system products which have been installed in hospitals and clinics internationally. This paper has been prepared as a formal testimony submission to the Senate Committee on Labor and Human Resources (chaired by Senator Kassebaum) and to the hearing proceedings to be held on November 14, 1995.

This document is the contribution of a private citizen and not the work of my employer. I have liberally included the thoughts and ideas shared with me by other members of the US healthcare medical informatics community. I bare sole responsibility for the content and any errors or omissions it might contain.

I offer the following suggestions and comments regarding U.S. Senate Bill S. 1360 - **'The Medical Record Confidentiality Act of 1995'**:

B. *EXECUTIVE SUMMARY*

There is a compelling need for legislation establishing uniform regulation of healthcare information disclosure and the rights of US citizens to protect their privacy. The absence of national regulation has been a major deterrent to improved security and confidentiality practices in United States healthcare provider institutions. While I believe that much of the content of Senate bill S. 1360 is good there are a number of conspicuous flaws which prevent me from supporting this Bill. Among them are five overarching issues:

1. There is no operational definition of the term 'personally identifiable health care information' yet this is a central concept to the act. Failure to clarify the meaning of this term renders the remainder of the legislation inoperative.

2. There is no distinction make between the usage & practice in direct care as opposed to external disclosure to individuals and organizations not directly involved in the care of the patient. I believe these distinctions are significant and must be addressed if the quality and cost effectiveness of services are to be maintained and controlled. The overarching issue is preserving the flow of information needed to deliver efficient and efficacious care to the patient while preserving the subject's right to privacy. Requirements during the course of care are not described explicitly. It is not clear if and how the requirements differ in these two rather distinct contexts.

3. There is no distinction made between electronic and paper records. There are fundamental differences in how the data is organized, accessed and distributed between the paper and the electronic form. The failure to qualify these distinctions is a major flaw and must be resolved in ordered to adequately address the unique requirements that are specific to each of the media in question (paper & electronic). Clearly the accelerating use of computers which is being encourage by our government exacerbates our exposure. We believe their is a compelling need to address the computerized context in specific.

4. Their is no concept put forward concerning the "chain of custody" requirements necessary to preserve the safeguards defined for the original trustee of the data. We need to insure that those that receive lawfully (or for that matter, unlawfully) disclosed data/information are held to the same standard as the originator.
5. There appears to be no provision that mandates even minimal levels of training for the recipients of confidential information or the documentation and retention of records of such training. Safeguards must be put in place to ensure that the 'trustees' identified in the act have adequately informed their employees/agents of their legal obligations under this legislation before further exposing them to confidential and sensitive health care information.

C. DETAILED ANALYSIS

1. SEPARATION OF HEALTH DELIVERY USE FROM EXTERNAL DISCLOSUE

Context: sec. 202 (a)

Issue: Internal (to the healthcare delivery organization) use is not separated from external disclosure. During the course of care the use of the record has been directed by an attending physician and primary care nurses who have been traditionally free to share it with colleagues who they believe can contribute to the care of the patient.

There is concern that these appropriate uses will require the consent of the patient in advance where none is required now and which would be found burdensome to the practitioners who have the interest of the patient in mind. The need to secure written consent for release of information would potentially delay appropriate and time-sensitive care.

Recommendation: Amend sec. 202 (a) to include the statement: ' internal use as approved by the attending physician and primary care nurses and for the purposes of consulting or for providing care' are hereby exempted from the disclosure authorization requirements of this section [sec. 202(a)].

2. *MEDICAL RECORD OWNERSHIP*

Context: sec. 201 (General Rules)

Issue: The bill does not clarify the ownership of the record itself. While putting in place safeguards for the patient and asserting their right to control external distribution of the record, the bill has not clarified that the institution or individual provider (in the case of a solo practitioner) retains the legal ownership of the record as a legitimate business record. The rights of both practitioners and healthcare institutions must be preserved if they are to defend themselves from malpractice lawsuits and other legitimate utilization of the records which they create.

Clearly the courts have upheld the originator's claim to ownership of the record. The thrust of this legislation might lead some to conclude the purpose of this legislation is to alter the current ownership. Clarification here might prevent such misinterpretation.

I believe the appropriate intention is to preserve the current ownership while asserting the special rights of the subjects of such business records. The need for legislation exists because such control over documents owned by another are not customary.

Recommendation: Amend sec. 201 (General Rules) introduce a new topic as part of paragraph (a) - ownership. Add the statement 'nothing in this act should be construed as altering or abridging the originators existing rights to ownership of the 'medical record' as a legitimate business record.'

3. *SPECIAL REQUIREMENTS IN THE CASE OF SELF-INSURED ORGANIZATIONS*

Context: sec. 111 (Establishment of safeguards)

Issue: Some concerns have found resonance in the healthcare informatics community. There are insufficient barriers to abuse by self-insured employers. While the need to validate claims for healthcare service payments is understood - how do we prevent employers from using the healthcare status of the employee to discriminate when there are potentially significant fiscal impacts on them (the employers) and where such abuse is very difficult to prove?

There must be a palpable & tangible "firewall" in place to block the surreptitious abuse of this information by lawful recipients such as employer.

Recommendation: While I don't have a specific suggestion as the language to provide the "firewall" the failure to do so would persuade me and a significant number of my colleagues to oppose the bill. This language should be inserted in sec. 111 with specific text addressing the special considerations when the claims recipient has a lawful need for the record but where (by virtue of the employer being self-insured) there is a significant risk of conflict of interest, either by the recipient directly or indirectly by it's client who is the employer. It must:

- Clearly define a 'firewall' of physical and access security which prevents the employer from gaining knowledge of the continuing health status of a subject or the nature of the services provided which might in turn divulge the nature of the patient's condition and need for ongoing care.
- Restrict the access to individuals who have no other functions within the organization aside from claims adjudication. These individuals should be legally prohibited from contact with other employees outside of the claims administration functions in order to prevent incidental disclosure which might be used against an employee by an employer attempting to reduce their exposure to legitimate healthcare expenses or other discrimination identified in the 'Americans with Disabilities Act'.
- There should be extraordinary penalties imposed for abuse of this section to compensate for the difficulty in proving such abuse. My opinion is that a limit of greater than several million dollars should be explicitly allowed.

4. *DEFINITION OF 'REASONABLE' EFFORT TO CORRECT RECORD ERRORS'*

Context: sec. 102 (a) (3)

Issue: There is no definition as to what constitutes 'reasonable effort' to correct records previously lawfully disclosed to other parties under sec. 102 (a) (3). The cost of creating and implementing disclosure updates could be significant. There is no clarification of who pays for the cost associated with such re-transmission of corrected information. There is no time limit established from the date of original disclosure to restrict the re-transmission to recent usage cases or to cases where there is a known persistence to a previously disclosed record.

Recommendation: Amend se. 102 (a) (3) to include a statement asserting a time limit on automatic redistribution of corrected information to medical record recipients who have received a previous disclosure of the incorrect information within 12 months of the request for correction or where the subject makes a specific request to update an explicitly identified previous recipient as part of the request for correction.

5. *RE-DISCLOSURE AND DISTRIBUTION COSTS IN NON-COMPELLING CASES*

Context: sec. 102 (b) (4)

Issue: There is uncertainty about re-disclosure be compelled under sec. 102 (c) even if the requested correction request was found non-compelling. A malicious mental health

patient could cause a significant cost for a facility if such a re-disclosure is required in cases where the request for correction was found non-compelling.

Recommendation: Amend sec. 102 (b) to include item (4) - exemption from notification requirements'. Include the statement: 'Denied requests should be exempted from the correction notification requirements.

6. *COST FOR DISTRIBUTION OF CORRECTED DISCLOSURES*

Context: A new clause sec. 102 (a) (5)

Issue: A new clause indicating that the costs will be treated in a fashion consistent with sec. 101 (a) ... the last sentence is needed. Unless this issue is clarified the cost burden of corrections remains ambiguous.

Recommendation: Add a new item as sec. 102 (a) (5) - Costs of redistribution of corrected records. Add the statement: the individual (subject of the record) may be required to reimburse the trustee for the cost of re-disclosure of corrections unless proven to have arisen out of negligence on the part of the trustee. This issue to be arbitrated in the same manner as set forth in sec. 102 (d).

7. *EXEMPTION FROM WRITTEN NOTICE OF INFORMATION PRACTICES*

Context: sec. 103 (a)

Issue: Health information service (companies) are specifically excluded from sec. 103 (a) - written notice of information practices. The reasons for such exemptions are unclear. They should not be treated differently. I believe we should remove the exemption for MIB (Medical Information Bureau) and all the other health information service companies. They are explicitly in the business of reselling health information. They appear to be precisely one of the parties who have potential motivation to abridge the patient's right to privacy.

Recommendation: Remove the phrase ' other than a health information service' from the first sentence of sec. 103 (a).

8. *COMPOSITION OF THE HHS CONFIDENTIALITY ADVISOR GROUP*

Context: sec. 111(b) (ii)

Issue: The advisor group specified under sec 111 (B) (ii) does not identify system vendors or healthcare informatics professionals as parties to be included in the advisory group. Their experience and knowledge of what is practical is an important component & input to the process. Other interest groups have been named - these two groups should be named as well.

Recommendation: Add item sec. 111 (b) (ii) (V) Healthcare information systems vendors/suppliers who product systems which contain components of or the entire electronic medical record.

And Add item sec. 111 (b) (ii) (VI) Healthcare informatics professional(s), particularly from healthcare delivery (provider) organizations.

9. *RECORD OF DISCLOSURE REQUIREMENTS*

Context: sec. 112

Issue: The content of the disclosure record information is uncertain under sec. 112. If it must be maintained for seven years the volume of data retained could be significant, particularly when the data is not specified in the bill. I suggest that the data be limited to the organization name, requesting party or custodian, date of request, & phone contact number for the requesting party.

Recommendation: Add a new item in sec 112 (a) specifying the record of disclosure data requirements (new sentence) and that this record be made a part of the medical record itself, both in paper and electronic form.

10. *DISCLOSURE AUTHORIZATION EXEMPTION FOR HEALTHCARE PRACTITIONERS DURING PATIENT CARE ENCOUNTERS*

Context: sec. 201 (f)

Issue: As asserted earlier - I believe that disclosure by those practitioners, including doctors, nurses, and allied health professionals, engaged in delivering current care should be exempted from the disclosure authorization requirements. Such exemption should be included in sec. 201. To allay some fears - computers could be modified to include a notice screen interposed when a user performs a new logon indicating the confidential nature of the patient medical record and the users legal obligations. Doing so at the logon step should not prove too onerous. This kind of thing is done frequently in military systems which contain classified information. Just a kind and gentle reminder too keep well-intentioned people mindful of their obligations.

Recommendation: Add as a new item - sec. 201 (f) exemptions. Add the statement: 'practitioners, including doctors, nurses, and allied health professionals, engaged in delivering current patient care are exempted from securing a patient disclosure authorization so long as the recipient is informed of their legal obligation to preserve the confidentiality of the record and its contents when it contains protected, personally identifiable, health information.

11. *INDIRECT PATIENT CARE-RELATED MEDICAL RECORD ACCESS AND USAGE*

Context: sec. 201(b)(1)

Issue: This clause is sufficiently vague as to make me uncomfortable. The phrase 'purposes for which the information was obtained' is nebulous. It can be argued that the data was collected to provide care to that patient (subject). There are numerous secondary uses for the data which are supported currently. If you're a strict constructionist you might otherwise preclude other appropriate uses such as quality assurance, nosocomial infection surveillance, blood and tissue utilization review, and other secondary but important uses of the data by the healthcare delivery organization or public health entities. In these cases the identity of the subject can sometimes be important.

Recommendation: Either define this phase in sec.3 or provide a specific exemption for intra-institutional (care provider organization), and public health use in sec. 201(b)(1).

12. *APPLICATION OF THIS ACT TO CARE PROVIDER ORGANIZATIONAL USE OF ELECTRONIC HEALTH RECORDS*

Context: sec. 2 and throughout the draft of this act

Issue: My hunch here is the authors never intended this act to impact internal use of electronic records. There is no language identifying user access restrictions in the context of a electronic system within a healthcare delivery organization. If this is the case then it should say so in the scope statement.

Local electronic access requirements for disclosure purposes have not been addressed by this bill as presently drafted. sec. 213 indicates that the secretary (HHS) should promulgate standards for disclosure without defining what electronic disclosure means. Wow - that's a pretty big hole to leave in the middle of a heavily traveled highway (Please forgive the indirect reference to the NII, can't resist a good pun).

My position is that these requirements for electronic access and disclosure are important enough to define as part of the legislation rather than to leave it up to the secretary. The

bill is clearly too limited in scope without these clarifications. In fact, existing electronic systems permit broader and simultaneous use of the record which was not possible with a paper record. With a paper record, the physical security possible with a single paper record is a generally effective barrier to systematic abuse. I believe the risks are greater in this electronic new age by virtue of the very attributes that made such electronic systems appealing - they make systematic review of the electronic record more efficient and easier to use by a large number of simultaneous users.

I'm confident that the vast majority of system suppliers have acted quite responsibly and have imposes reasonably effective barriers to abuse - typically with multi-step logon procedures prior to allowing access. The question here is should legislation be enacted without explicit treatment of this issue.

For instance should an electronic system enforce restriction of access to the record to only those physicians with a pre-established care-role relationships to the subject. What about nurses who provide care to patients at a local or nursing unit or home care region. What about those with legitimate system-wide patient access requirements such as nosocomial infection surveillance officers and nurses. I personally subscribe to the notion that capturing a self-authenticated relationship (role) of the user to the subject is a good solution. If retained as part of the record this should serve as an adequate protection - one which could and should be policed by the care provider organization.

Recommendation: in sec. 2 as a new item ... say item (4) assert what is not intended to be covered by the act.

13. *SPECIAL CONSIDERATIONS FOR REMOTE ACCESS TO ELECTRONIC MEDICAL RECORDS*

Context: Not specifically covered by this act.

Issue: Remote access exposes yet another issue in the electronic age. With modern interface tools such as Microscript's ™ "screen scrubber" utility, a remote user can easily transfer the entire content of a prolonged query dialog to their remote computer setting - one no longer controlled by the trustee. If the remote user had appropriate access authority the system supplier and trustee should not be held accountable. I believe that any legislation should clearly identify the liability of lawful users who use the data for unlawful purposes. Restricting the liability to the user which knowingly executed unlawful use of their access authority is critical.

Recommendation: I would suggest that sec. 301 (Civil Penalty) should be modified to include a new sec. 301 (c) exemption of liability for the trustee in cases where an unlawful use is knowingly committed by an agent/employee without the knowledge or consent of a trustee and where that use was in direct violation of the trustee's written policies (with evidence that the employee/agent did receive training and had signed a statement acknowledging their legal responsibilities) and where appropriate action to sanction or correct their employees behavior have been demonstrated by removal of privileges and employee sanctions up to and including termination. This act should recognize such behavior as a termination-eligible offense.

In order to prevent more surreptitious abuse... where it can be demonstrated that the employer coerced or otherwise enticed the employee or agent to engage in unlawful behavior - the maximum civil penalties should be tripled! ... say up to six million dollars per offense. Sec 311(b)(3)penalties are presently limited to 500k which is too low in my opinion). These measures should create sufficient exposure to limit systematic abuse by business organizations or employers of any size. I'd say, for the purposes of this legislation, that payment above and beyond the standard compensation for their normally defined duties for unlawful acts or the transfer of such unlawful information constitutes employment (the intention here is to catch "temps" or informally hired computer hackers and remove the shelter that might otherwise be afforded their employer).

14. *CHAIN OF CUSTODY AND LEGAL RESPONSIBILITIES.*

Context: The entire document

Issue: Nowhere in the document is the concept of the chain of custody and accountability established. Much like the existing legal requirement for each party in the chain-of-evidence to maintain the integrity of the material, there is an equal need to ensure that each party receiving material under this act is individually accountable to preserve the confidentiality of said material to at least the same extent as was required of the original source of the record and further limited by the terms of disclosure authorization agreement by which the material was obtained. In other words, the third hand recipient is bound by the original release authorization unless a newer one is obtained. In no case should tertiary recipients abridge the patients rights and be held less accountable because the secondary recipient failed to stipulate the conditions of the release of information contained in the original authorization. It might be a good idea to mandate that the patients (subject) authorization become an essential part to the released material whether in paper or electronic form. Each recipient should also be required to update their records upon receipt of a correction from the original trustee.

Recommendation: Added a new topic to sec. 201 (f) (General Rules) addressing this issue. Maybe something like the phrase 'each and every recipient of identifiable health information is bound to the terms and conditions of the original patient's (subject) authorization for the release of said information and to update their records upon receipt of any corrections to the original disclosure information. Said corrections should be clearly marked and should preserve the succession of results and time for each result or fact. The content of the original disclosure authorization should be retained as part of the record.'

Consider adding the statement 'Any violation of these terms or other legal obligations should be reported to the organization holding the original record within 2 business days from the date of obtaining knowledge of such a violation.'

15. *REQUIREMENTS FOR TRAINING AND TRAINING DOCUMENTATION IN THE APPROPRIATE USE AND OBLIGATION TO SAFEGUARD MEDICAL RECORDS*

Context: the entire act

Issue: Nowhere in the act are requirements levied to provide and document training to employees/agents of holders of medical records. In order to make this act enforceable a large number of persons will require education and training. Such material and training should be stipulated for all those individuals granted access to such record. The definition of the precise details could be reasonably assigned to the secretary (of HHS).

Recommendation: create as section ... say sec. 214 (Training Requirements). Assert both education and documentation requirements.

16. *DEFINITION OF THE TERM 'PERSONALLY IDENTIFIABLE HEALTH CARE INFORMATION'*

Context: the entire act, especially sec. 3 (definitions)

Issue: There is no operational definition of the term 'personally identifiable health care information' yet this is a central concept to the act. Failure to clarify the meaning of this term renders the remainder of the legislation inoperative. I believe that there is no clear consensus for the meaning of the term. At the two ends of the polemic are: identifiable means all of the content taken together or a significant subset because the medical facts when assembled together would allow one to discriminate among persons to yield a very small subset or even a single person (as in a series of dates the person came to receive ambulatory care and their blood type). At the other end of the spectrum are those that limit identifiable to mean person name and address and nothing else.

I favor an intermediate position which I would characterize as reasonable rather than heroic. I believe we must remove basic demographics including the name, address, phone numbers, uniquely or semi-uniquely assigned social security numbers, health insurance plan identifiers, state drivers license number, and all similar information on parents and next of kin contained in the record in order to suggest that it is no longer identifiable.

By the same token I would like to explicitly retain date-of-birth, postal (zip) code, and gender (sex) as useful data when compiling population statistics. The presence of date of birth and gender should not be construed as identifiable when the items listed above in the preceding paragraph have been removed.

Recommendation: that sec. 3 (definitions) add a definition for the term 'personally identifiable health care information'. I suggest my definition list above: 'personally identifiable health care information' means and record which contains among other data and of the following elements: the name, address, phone numbers, uniquely or semi-uniquely assigned social security numbers, health insurance plan identifiers, state drivers license number, and all similar information on parents and next of kin.

17. *PROTECTION OF PRACTITIONERS AND IDENTIFIED SOURCES OF MEDICAL CONTENT WITHIN THE MEDICAL RECORD*

Context: the entire act,

Issue: There is no provision to limit the disclosure of the identity and personal information of practitioners and other sources of information contained within the medical record. It is not unusual to find references to contact information about individuals involved in the care of the patient either directly or indirectly. It is likewise not atypical to specifically identify a private citizen who has contracted a communicable diseases from a subject or whom the patient contracted the disease from. These references are often contained in progress notes embedded as free text. Some effort should be taken by the trustee to obscure identifiable components or obtain their permission to disclosure prior to the release of information.

I favor the removal of this information or obscuring the content sufficient to render it non-identifiable.

Recommendation: Add to sec. 201 (General Rules) protection for practitioners (doctors, nurses, and allied health professions) and other individuals named or otherwise identified within the content of the medical record. Provide that their identifiable information is removed or their permission is obtained in a manner equivalent to sec. 202 (Authorizations) prior to information disclosure.

STATEMENT OF THE AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS

In the past decade the confidentiality of medical records has been severely eroded by several developments: the increasing demands of insurance companies for clinical information, the increasing computerization of medical records (which has made these records more easily accessible to large numbers of people), and, more recently, the corporatization of health care (leading to increasing demands for data to assist with business decisions). Corporate America, which has never manifested a high regard for personal privacy, is involved in all of these developments. It currently advocates a shift from paper-based to completely computer-based medical records. Indeed, it portrays this shift as inevitable and as a cost-saving measure.

The ACLU of Massachusetts believes that these developments are fraught with peril for patient rights and for the quality of American medical care and research. While the shift to computer-based records may yield some improvements in efficiency, we see little convincing evidence that it will in general result in cost control. We are certainly not opposed to all uses of the com-

puter in medical care. We only believe that this tool, like all others used in medicine, must be rigorously evaluated with respect to its appropriateness for various tasks. (For an overview of the problems posed by the computerization of medical records, see Beverly Woodward, "The Computer-Based Patient Record and Confidentiality," New England Journal of Medicine, Nov. 23, 1995.)

S.1360 has been represented by some of its sponsors as an effective response to the threats to medical record confidentiality mentioned above. However, a close study of the bill has convinced us that this is not the case. We would welcome stringent federal legislation to protect medical record confidentiality and patient privacy, but this bill does not provide that. In what follows we shall discuss some of our concerns.

S.1360 is designed to facilitate the shift from paper records to computerized records and to remove the obstacles to the flow of patient-identified information across state lines. To achieve this, it preempts the state statutes that provide general medical confidentiality protection and common law pertaining to medical privacy. In so doing it nullifies a large part of the tradition of tort law redress for privacy violations that was initiated by the famous Brandeis/Warren article on "The Right to Privacy."

The bill places responsibility for control of access to patient records in the hands of "health information trustees" (generally institutions) rather than attempting to return it to the hands of patients and their physicians. It permits widespread access to patient information within health care institutions (insider access) and authorizes access, without patient consent, by public health departments, health care oversight agencies, medical researchers, health information services, law enforcement personnel, and parties armed with subpoenas. (Secs. 204-212) We believe that these permissions will make those provisions of the bill that protect confidentiality relatively ineffective.

The bill fails to acknowledge or take into account the special problems with respect to maintaining confidentiality in computerized systems. Because computerization enables the collection of vast amounts of data and rapid access to such data, it facilitates the rapid theft of data (sometimes in large amounts) as well as improper viewing on a grand scale. Computerized record systems pose new temptations and new opportunities for illicit activities.

In addition, the use of computers for storing patient medical information tends to eliminate the kind of case by case judgments with respect to disclosure of information that in the past were the responsibility of medical records professionals and of primary care physicians. While this defect might be overcome, if all the information were encrypted and only the patient and a few others were given the authority to decrypt, there does not appear to be the will to move in this direction.

Insider access: The bill, taken as a whole, sidesteps the problem of insider access to medical records. Yet computer experts state that the vast majority of violations of confidentiality are due to the actions of insiders (rather than "hackers" on the outside). As a result of the merger mania prevalent in the healthcare industry at the present time,

insiders in some health care networks and corporations number, or may soon come to number, in the tens or hundreds of thousands. It is more and more the case that the "outside" is being brought inside. Insurers are combining with providers, pharmaceutical companies with HMO pharmaceutical prescription management corporations, etc. It is now common for a corporation that seeks information held by another entity to buy out or form a strong contractual link with that entity.

The bill contains only a few provisions that pertain to the problems of insider access. It states that "a health information trustee shall establish and maintain appropriate administrative, technical, and physical safeguards to ensure the confidentiality, security, accuracy and integrity of..health information..." (Sec. 111) This very general provision leaves it to the health care industry to regulate itself and fails to prescribe any means by which the stated objectives are to be achieved.

The requirement that disclosures within a health care system or institution be "compatible with and related to the purposes for which the information was obtained" (Sec. 201) fails to acknowledge that information may be obtained by health care providers for reasons quite different from the reasons why patients reveal information. The business purposes of a health care provider, for example, may have nothing to do with the patient's objectives in seeking health care. The bill permits health information trustees to share information as they deem necessary with employees, contractors, affiliates, and subsidiaries. ("Frequently Asked Questions," a document available from Senator Robert Bennett, hereinafter referred to as FAQ, #12) Many hospitals and networks presently are permitting thousands of persons to have easy access to the records of all of their patients.

The "minimum disclosure" provision (Sec. 201) gives the "health information trustee," not the patient, the power to decide what minimum disclosure is. In fact, most hospitals and health care networks are now putting, or intend to put, the patient's <u>entire</u> medical record online. They rationalize this practice by saying that the entire record may be needed quickly in a medical emergency. (Many physicians, however, are of a different opinion.) Given the fact that the supporters of this bill state that "many hospitals and doctors are already mostly in compliance" with the bill, there appears to be no intention to regulate and limit disclosure within hospitals and health care networks. (FAQ, #22)

The "accounting for disclosure" provision requires only that health information trustees keep records of disclosures <u>not</u> related to treatment. There is no requirement that health care providers keep an audit trail of internal electronic disclosures, or that employers keep a record of who has seen an employee's medical records, or that schools keep a record of who has looked at a student's medical information.

<u>External disclosures</u>: The bill has provisions for obtaining patient consent for certain disclosures by health information trustees to outsiders. For example, consent must be obtained for the release of medical information to a school or for release to an insurance company. (However, these latter "consents" are not freely given, since they <u>must</u> be given in order to have medical bills covered.) The bill also contains an imposing list of disclosures for which consent is not required. (Secs. 204-212). These include disclosures to public health agencies, health information services, medical researchers, health care oversight

agencies, law enforcement personnel, and persons armed with subpoenas. We believe that these exceptions are either quite unnecessary or overly broad. A computer security consultant to the British Medical Association reviewed this bill and was astonished at the scope of these provisions. (Letter attached.)

The sections on law enforcement are especially alarming to civil libertarians. Included are provisions that would permit a government authority that is inquiring "into a violation of, or failure to comply with, any criminal or civil statute or regulation, rule or order issued pursuant to such e statute" to obtain by subpoena or warrant personal medical information that is judged "relevant" to the inquiry. This would appear to open the door to obtaining medical information about almost anyone. The requirement that the information merely be "relevant" is much weaker than the current Fourth Amendment requirement for a search, namely that there be probable cause to believe that a crime has been committed and that the target is guilty of the offense. Given the intimate details in many medical records, a weak standard is not acceptable.

Another provision in the law enforcement section would open the door to wide-ranging police inspection of medical records, including trolling through large computerized medical record data bases, when a legal offense or suspected offence had occurred on the premises of or in connection with a health care provider or when the police were attempting to identify a witness or victim. These broad provisions can easily be used to invade the privacy of patients unnecessarily.

In general, we may ask, "Who will decide what releases of information are necessary for an investigation? The police? How can it be determined and who will determine whether an investigation is based on real evidance already obtained or is merely a fishing expedition?" Any health care provider can be put in a difficult situation, if the police arrive and announce that they need to go through their records for such a purpose.

Under the bill medical records can also be obtained by non-law enforcement subpoenas. Such subpoenas will be upheld if a court determines that there is "reasonable" ground to believe that the information sought is "relevant" to a lawsuit or other judicial proceeding and where the "need of the respondent for the information outweighs the privacy interest of the individual." This kind of language has become increasingly common in privacy legislation, but that does not make it satisfactory. It will always be difficult to protect individual privacy, if privacy is termed an "interest" and not a fundamental right.

<u>Research, oversight, public health surveillance</u>: The bill makes no attempt to set strict controls on access to patient-identified information for research, health care oversight, or public health surveillance activities. Public health and health care oversight agencies will get patient-identified information without patient consent and without any review of the merits of the research or of the need for patient-identified information.

Researchers affiliated with hospitals and academic institutions, however, will have to go before institutional review boards to justify their need for patient-identified information.

We have reason to fear that in a computerized environment the review boards will not set a high standard in deciding which abrogations of medical record confidentiality are "justifiable." A growing number of health care administrators view all medical records, particularly computerized records, as research tools that can be used in the future for countless studies of "outcomes," "cost effectiveness," etc. Although there is no consensus among medical researchers and economists about the validity and usefulness of such studies and others that would link medicine and social science, S.1360 would facilitate the transformation of patient records into documents used as much for statistical research and business analyses as for patient care.

Health information services (HIS): The bill sanctions the creation of a new kind of entity in the health care field, the health information service (HIS). (Sec. 3, 1&6, Sec. 204) Health information services that create "nonidentfiable health information" will receive identifiable information without patient consent. (Sec. 203) The bill does not spell out how this identifiable information will be transmitted, what will happen to it once it is in the possession of a HIS, how long and in what form it will be retained, whether it will be used to create longitudinal "nonidentifiable" information, etc.

The health information service concept in this bill runs counter to generally accepted standards for protecting confidentiality. In Britain, for example, "if records are to escape confidentiality controls on the grounds of anonymization, then this must be done by the clinician before they are released, rather than by the recipient." (See attached letter.) The transmittal of identified information to data processors--the HISs--facilitates the creation of comprehensive records on individuals (which would not occur, if the identifiers were removed prior to release of the information) and the creation of inclusive regional data banks. We know that these are the ultimate goals of the supporters of this legislation. (See The Computer-Based Patient Record: An Essential Technology for Health Care, Institute of Medicine, 1991 and Health Data in the Information Age: Use, Disclosure, and Privacy, 1994; both are reports of the Institute of Medicine published by the National Academy Press, Washington, DC.)

Although the information in comprehensive data banks can be used for beneficial research, it can also be used in ways harmful to individuals and groups. Moreover, no matter what security measures are adopted, such data banks provide tempting targets for intruders and data thieves. Given the potential for harm, the ACLU has generally opposed the "computerization of manual record systems of personal information by government or commercial bodies unless proper standards and safeguards for privacy and due process are first provided. (Emphasis added.) This bill does not provide such safeguards, but leaves this to a vague process involving HHS.

Because health information services will be collecting comprehensive information on individuals and in some cases will be able to release this information without patient consent--to medical researchers, law enforcement officials, and public health agencies, for example (Sec. 3, Sec. 204), the HISs will facilitate forms of health surveillance that are unprecedented in this society. The decision about establishing such databanks should not be a decision made by the computer, information processing and health care industries, but a decision made by the citizens of this country after extensive public discussion.

In response to the question "What is the cost of this legislation?" its supporters have written "There is no CBO cost estimate yet." Whatever the economic costs, we believe it essential to factor in the mental anguish that millions may suffer if this bill is passed, the damage to personal control over personal records and medical decision making, and the discrimination that may result as the information in medical records becomes more widely available.

STATEMENT OF JAMES BRADY

Gentle Readers: I agree that legislation is needed to protect confidentiality of medical records; I would like to believe it would be better left to the States, but must agree with those that contend that the States have failed to adequately promulgate such legislation. And with our mobile society frequently crossing state lines, the present patchwork of protection or lack of protection among the States makes meaningful protection to the individual nonexistent. Although the Bennett Bill can not be the panacea for all problems in the medical information area, it appears to address most of them.

There are some areas not specifically addressed that perhaps could be worked into the bill. The areas comes into play when a life or health insurance policy claim is triggered within the contestable period, usually two years. Many hospitals and many doctors contend that the INFORMATION and the MEDIA upon which the information is stored belong to them! The more enlighten person contends the INFORMATION belongs to the PATIENT and the MEDIA to the provider; I agree with the latter position.

I have been an insurance investigator for almost 23 years. I repeatedly witness claiments needlessly suffer delay and insurance companies needlessly suffer unecessary costs because:

1) the trustee of the patient's health data refuses to permit the claimant authority to decide how long the authorization shall be valid and the trustee demands that it can dictate how long the authorization shall be valid even though such demand may and can work an onerous disservice to the beneficiary of the policy. THE BILL SHOULD MANDATE THAT THE INFORMATION BE CONSIDERED OWNED BY THE PATIENT AND THAT THE PATIENT HAS THE RIGHT TO CHOOSE THE PERIOD OF VALIDITY.

2) the trustee of the patient's health data refuses to permit the claimant and insurance company authority to best utilize the company's staff or a third party investigator and said trustee insists that the claimant must delineate the EXACT business entity if there be a third party, notwithstanding the fact that on a given claim the insurance company may choose more than one third party vendor. Such a demand frequently delays claim work and increases the cost of doing business to the company. The company may not know the identity of the vendor it will use when the claim is first presented. THE BILL SHOULD MAKE IT CLEAR THAT THE TRUSTEE HAS NO AUTHORITY TO STEP BETWEEN THE INSURED AND THE INSURANCE COMPANY AS IT PRESENTLY DOES.

3) the trustee DEMANDS the next of kin or beneficiary go to the needless expense of getting an executor or administrator of an estate that is either insolvent or extremely small solely to have an executor's or administrator's signature on the authorization of a deceased patient when the next of kin's or beneficiary's signature is quite adequate. THE BILL SHOULD PREVENT TRUSTEES FROM MAKING SUCH DEMANDS AND ALLOW NEXT OF KIN, POLICY BENEFICIARY, OR OTHER REPRESENTATIVE TO SIGN AN AUTHORIZATION FOR A DECEASED PATIENT'S HEALTH DATA.

STATEMENT OF THE CONSUMER PROJECT ON TECHNOLOGY

The following comments of the Consumer Project on Technology (CPT) outline our suggestions for improvements in S. 1360, the Medical Records Confidentiality Act.[2] While we join others in applauding the sponsors of S. 1360 for focusing attention on the important issue of privacy of medical records, we cannot support the bill as introduced. Our initial concerns about S. 1360 are detailed in an earlier November 2, 1995 letter, which is attached. I will briefly summarize our objections the legislation, and then detail specific areas where we think S. 1360 can be strengthened.

As introduced, S. 1360 does more to protect the medical records industry than the privacy of patients. The legislation severely limits state action on medical records privacy issues. Consumers lose rights to sue health care trustees under common law. Insurance companies, employers or HMO's have the right to demand access to medical records as a condition of payment. Once records are acquired by the Insurance company, HMO, or self insured employer, there are literally millions of persons who have the right to obtain the records, without the consent of the patient.

S. 1360 defines law enforcement investigations extremely broadly, to include more than one millions persons involved in enforcement of any civil or criminal statute, regulation, rule, or order.[3] Law enforcement officials will have access to medical records without consent or even prior notice, and will be permited to use computer databases of records to search for persons whose identity is unknown, including witnesses, suspected wrongdoers, or anyone who is "relevant" to an investigation.

Health care researchers, including those not affiliated with universities or hospitals, public health officials, health oversight officials, and other groups are given access to patient records, without consent or even notice. While health information trustees are required to keep records of persons who have access to records for non-treatment purposes (for seven years), patients will likely find it extremely difficult to locate these records.

Health care providers, insurance companies, large employers, computer and information services companies have successfully lobbied to obtain provisions that protect their commercial interests. Government agencies, such as the law enforcement community, and the health care "research" community have also successfully asserted extremely broad claims of access to medical records. As a result, S. 1360 is framed more as an access bill, than a privacy bill.

Under S. 1360, large systems of computer databases with cradle to grave medical records will be easily available to anyone with access. Records need not be stored in centralized databases to be readily accessible. Different databases, which are managed independently, and stored in remote locations, can be linked together by telecommunications networks, and used in a manner similar to a single database, if queries can be delivered and authorized electronically, as is allowed and anticipated under S. 1360. The amazing efficiencies of new information technologies are being combined with equally important revolutions in medical technologies. Basic information about weight or blood type are being supplemented by data on genetic characteristics and other high-tech items. It is not enough to write rules which largely codify current practices, with cosmetic improvements.

Firms with access to medical records databases are investing in product development and marketing strategies, in order to encourage greater access to the medical records, not less access. Self insured or experience rated employers will be encouraged to study records in a variety of ways to manage health care costs. Insurance companies will be encouraged to run medical audits, with "consent," before issuing policies. The huge numbers of law enforcement officials with access to medical records will be a market, waiting for the development of the right "products" to enhance the efficiency of their investigations. S. 1360 will facilitate the development of those markets, because it largely removes doctors from the role of guardians of patient records, and it does not question the right of large businesses to build systems which allow for automated searches of personally identifiable patient records.

Some proponents of S. 1360 claim that the bill will enhance privacy, because current laws and protections are so weak. The "something is better than nothing" argument would be more persuasive if the law did not preempt state action, or eliminate privacy law suits under common law. "Something" is hardly the appropriate response to the problem at hand. Without real privacy protections, consumers will withhold information from doctors, and doctors will create untruthful records, in order to avoid the transmission of the information to a system that is so porous.

The following are suggestions for language which would increase the level of consumer privacy.

1. Doctors Should Exercise Greater Control over Records.

Under S. 1360, an entity that pays for medical care may require disclosure of protected health information [Sec 202 (a)], and the authorization to obtain health care records to validate expenditures may not be revoked [Sec 202 (b) (1)]. This is an important step in the process, because if the entity that pays for the treatment obtains the records, decisions about disclosure of the data will be made by persons other than doctors responsible for treatment.

Some advocates of S. 1360 say that one can avoid having medical records entered into large databases by paying out-of-pocket for health care costs. For consumers who struggle to make ends meet, this is not a particularly viable option. Privacy of medical records should be available to everyone, regardless of income.

We suggest a new subsection 202 (e), which states:

Sec. 202 (e) Disclosure for Payment. -- A health information trustee that receives protected health care information for purposes of authorization of payment may only use information for this purpose, and may not redisseminate the information to any third parties, including persons who seek information under sections 204, 205, 206, 207, 208, 209, 210, 211 or 212 of this act. Protected information received for purposes of payment authorization shall be removed or destroyed at the earliest opportunity once payment has been authorized.

2. The Preemption of State Law Is Too Broad.

The Sec. 401 preemption of state law is far too broad, and results in the legislation acting as a ceiling on privacy, rather than a floor.

Sec. 401 (a) states that "except as provided in" certain areas, "this Act preempts State law." The exceptions include:

- state law on the privileges of witnesses, vital statistics, records on abuse or neglect of an individual, public or mental health records, rights of minors to medical records,
- the provisions in the Public Health Service Act relating to notifications of emergency response employees to exposure to infectious diseases,
- federal law governing confidentially of alcohol and drug patient records,
- the Americans with Disabilities Act of 1990,
- Federal or states law which establishes a privilege for records used in peer review activities.

I would suggest striking this section altogether. If this isn't possible, add a new section (c) (9), to add another item which S. 1360 does NOT preempt.

> (9) any State law which limits the collection, indexing, dissemination, or maintenance of medical records in electronic formats.

As you know, we are concerned S. 1360 does not take adequate account of the impact of computer technologies on privacy, and that the fact that records are stored in digital formats creates new threats to privacy. By adding our proposed (c) (9) to Sec. 401, states will be free to enhance the baseline privacy protections of S. 1360, by addressing the most important issues in the management of the records in electronic databases. Some state legislatures may decide that their citizens deserve greater privacy protections than those that are included in S. 1360. We see no reasons to deny state action in this area.

3. Congress Should Not Take Away a Citizen's Right to Sue under Common Law.

Under Sec. 402, a health information trustee (which includes just about anyone who manages or uses these records), and who makes a disclosure about an individual "that is permitted" by the Act, shall "not be liable to the individual for such disclosures under common law." **This section should be stricken.** There is no need to provide this super immunity to the health information trustees. They retain broad discretion under the law, and health care consumers should have the right to pursue their rights under common law for violations of privacy. Under Section 201 (c), the bill says that "nothing in this title that permits a disclosure of health information shall be construed to require such disclosure." The Sec. 201 (c) language is important, because it underscores the fact that health care providers and health care trustees have the discretion *and* the responsibility to limit disclosures of information to protect privacy. S. 1360 is written to address all possible uses of medical records, and consequently, it gives quite broad authority to disseminate information. However, consumers expect that health care providers and health care trustees will exercise reasonable judgement in making decisions about when to disclose. The elimination of common law rights of action is an unwarranted and unnecessary elimination of an important incentive for health care providers to use caution in authorizing disclosures.

4. The Law Enforcement Provisions Are Absurd, and must Be Vastly Narrowed.

As noted in our letter of November 2, 1995, we are alarmed at the seemingly wide open provisions for law enforcement access to medical records. This term the United States Supreme Court is considering a case where a law enforcement official is asserting that her mental health records should be privileged, and not made available to the government. Most Americans believe that their own medical records are privileged documents, not subject to easy perusal by law enforcement officials. We estimate that well over 1 million government employees will have the right to access to medical records under S. 1360, without consent or prior notice, under the very broadly defined Sec. 212 law enforcement provisions.

This section gives any government official who is responsible for enforcement of any criminal or civil statute, or regulation, rule or order adopted under the authority of a statute, access to medical records. It is written in such a way that even a dog catcher or building inspector will have the right to obtain a warrant for access to a person's medical records. Congressional staff appear to be covered as well.

Law enforcement officials are given the right to obtain records for persons whose identities are unknown, or to use medical records databases to identify witnesses or victims. The only standard for access is that there must be probable cause that the information is "relevant" to an inquiry -- even if a person isn't the target of the investigation. Will the police obtain medical records in order to prepare for an interrogation or questioning of acquaintances of suspected

wrongdoers? Will this become standard procedure when putting political dissidents under surveillance? What would this have done for Nixon's plumbers when they sought "access" to Daniel Ellsberg's psychiatric records?

The following are initial suggestions for reducing the problems in Sec. 212.

- The definition of a law enforcement inquiry must be significantly narrowed.

- Government agencies that obtain medical records under the law enforcement exemptions should be required to publicly disclose the number of warrants or subpoenas for medical records obtained every year, the names of the employees who received the information. This will provide an important deterrence, and some mechanisms for accountability.

- Law enforcement officials should not have the right to obtain mental health records under warrant or subpoena.

- The law should severely limit the ability of law enforcement officials to use computer databases to search for and receive medical records. It would be better if the law enforcement official was required to obtain the records from the doctor, to give the doctor the opportunity to resist, if the doctor believed it was important to refuse access for ethical reasons. Law enforcement officials should not be allowed to search databases for unknown persons. This gives rise to frightening scenarios for surveillance, and it should be rejected now, before we begin the process of even greater accumulation of knowledge about genetic characteristics and other information.

- Law enforcement officials should be flatly prohibited from obtaining protected medical records information for purposes of building psychological profiles, investigating acquaintances or colleagues, or other clear abuses.

- Persons should have a right of action to sue law enforcement officials who seek overly broad information, or health care trustees who disclose too much information.

5. Consumers Will Find it Difficult or Impossible to Locate the Records Which Account for Disclosures. Much Can Be Done to Improve Sec. 112.

Under Sec. 112, a health information trustee will be required to create and maintain records of disclosures that are not related to treatment, including the many types of disclosures allowed under Sections 204, 205, 206, 207, 208, 209, 210, 211, and 212. These will be extremely important data, because they are one indication of how often our medical records are shown to others. For 7 years this data will be considered protected health information. [Sec. 112 (b)]. Under Sec. 101 (a), it appears as though a consumer is entitled to inspect or copy these records, since the consumer is "the subject" of the protected information. However, locating this information will be difficult. Health care trustees will maintain the disclosure records in remote locations. Under Sections 204 through 212 there often be no notice to the consumer that a disclosure has occurred. In order to discover that a disclosure has been made, a consumer will have to contact health care trustees, one by one, making inquiries. A failure to report a disclosure at any step will eliminate the record trail. Health care trustees have 30 days to respond to requests for information, and one can anticipate slippage in that number. The trustee can require the consumer to pay for "the cost of such inspection and copying." One can imagine a fee charged simply to make an inquiry. It seems likely that an exhaustive search of trustees that may have had access to ones records could take years and hundreds or thousands of dollars, every time it was undertaken. Indeed, it could be much more difficult, when one considers the fact that one's entire medical history, from cradle to grave, is involved. This greatly diminishes the usefulness of the records. We are also concerned that some health care trustees will simply not report the Sec. 112 disclosures at all, leaving gaps in the record trail.

Proponents of S. 1360 say that it is enough to give the consumer a record trail, which shows directions where one might look. We would like to see each user of a patients record report back to the source, every time the record has been accessed. If the trail can lead one way, it surely can be designed to lead the information back in the direction where the consumer might actually find it. To accomplish this, we recommend adding the following new subsection (c) in Sec. 112.

> Sec. 112 (c). The health care trustee shall provide copies of records of disclosures to the person who maintains custody of the original copy the protected health care record, and that person shall attach the report to the original record.

We were also surprised to see that the length of time that the health care trustee must maintain its records has been shortened from the 10 years that appeared in the copies of S. 1360 disseminated by Senator Bennett on the bill's introduction, to 7 years in the printed version of the bill. [Sec. 112 (b)] We prefer a longer period, twenty years.

We are also in favor of a provision that requires health care trustees to report data on disclosures to a centralized location, so that we can see statistics on how often consumers records are accessed, and for what purposes. The Secretary should adopt rules for reporting this information, for all health care trustees, providing statistical data on the number of times records are accessed, who obtains access, under what sections of the law was access obtained, and for what purposes was the information used. We recommend a new subsection (d) be added to Sec. 112, which says:

> Sec. 112 (d). The health care trustee shall provide annual statistical reports to the Secretary, in a format which is specified by the Secretary, which discloses the number of records that are accessed, the types of persons or entities who obtain access, the sections of the law under which access was obtained, and the purposes for whcih the information was used. The health care trustee shall also obtain an independent audit to verify the information provided in this report. The Secrerary shall make these reports available to the public.

6. The Consent Section Should Be Strengthened, to Limit Cases Where "Consent" Is Obtained with Coercion.

The Section 203 provisions for disclosure for purposes other than treatment or payment are based upon the fiction that consent will occur without coercion. Today it is common to be asked for "consent" for access to medical records in order to obtain life insurance. Under S. 1360, we anticipate a growth in services for searching medical records after obtaining consumer "consent" agreements. We are concerned that employees will seek "consent" to examine medical records, in order to estimate the cost of providing medical benefits, or to search for other information, such as evidence of homosexuality, mental illness, sexual promiscuity, or deviant behavior, to list just a few items.[4] With a huge industry built around the maintenance, transfer and indexing of patient records, it will increasingly become easier to conduct such searches. If employers are allowed to request "consent," it will be difficult to refuse. Indeed, a refusal will be a signal that the employee has something to hide.

The consent section should be strengthened by including a provision 202 (e), for rules against coercion, which states:

(e) The Secretary, after notice and opportunity for public comment, shall adopt rules which prohibit or limit requests for consent for access to protected health care information for purposes of employment, acceptance to a school or university, or for other purposes for which a request for consent may involve undue coercion.

If this Congress is unwilling to protect the public from requests for consent under coercion, then a provision should added to section to Sec. 401 (c), stating that this is an area where states are not preempted from acting.

Sec. 401 (c)(10) Any state law that limits the right of employers or other groups to request consent for protected medical information.

7. The Provisions for Access by Health Oversight Agencies [Sec. 207], Public Health Authories [Sec. 208], and Health Researchers [Sec. 209] Should Be Modifed to Require Notice in Every Case. Consent Should Be Required in Most Cases. Addditional Reporting Is Needed.

At present, health oversight agencies, public health authorities or health reasearches have the right to access medical records without consent and without notice. This presents far too much access to medical records, and not much in the way of accountablity. For each group, notice to consumers should be required. In cases where consent is not obtained, the notice should include at least the following information:

(1) the records to be accessed,
(2) the reason for obtaining the records,
(3) the legal authority under which the records were obtained,
(4) the names of the persons who have access to the records, and
(5) how the records will be used, including disclosure of the length of time the records will be in the possession of the person obtaining access to the records without consent.

Health researchers should be required to obtain consent to receive access to records with personal indentifiers.

Since we don't know much about how these groups use medical records, or how that usage is changing as records are becomming computerized, we need annual reports which provide statistical information. These reports should be made pubic.

> Sec. 112 (d). The health care trustee shall provide annual statistical reports to the Secretary, in a format which is specified by the Secretary, which discloses the number of records that are accessed, the types of persons or entities who obtain access, the sections of the law under which access was obtained, and the purposes for which the information was used. The health care trustee shall also obtain an independent audit to verify the information provided in this report. The Secretary shall make these reports available to the public.

The Consumer Project on Technology has created an Internet discussion list for this issue, called **med-privacy**, which available for subscriptions from listproc@essential.org.[5] Our World Wide Web page has additional information, and is located at:

http://www.essential.org/cpt/privacy/ptivacy.htm.

---

[2]The Consumer Project on Technology (CPT) is a project of the Center for Study of Responsive Law. The CPT was created by Ralph Nader this year to study a number of issues related to new technologies, including telecommunications regulation, pricing of pharmaceutical drugs, intellectual property rights, and the impact of computers on privacy. The URL for our home page is: http://www.essential.org/cpt/cpt.html.

[3]For example, the Department of Justice estimates that in 1992 some 841,099 persons were employed by state and local police and sheriffs departments.

[4]Employers are limited in the information they can request about medical records prior to employment, under the federl Americans with Disabilities Act of 1990.

[5]Send a note to listproc@cap.org, with the message:
subscribe med-privacy yourfirstname yourlastname

STATEMENT OF THE HEALTH INDUSTRY MANUFACTURERS ASSOCIATION

The Health Industry Manufacturers Association (HIMA) is pleased to submit the following comments regarding the Medical Record Confidentiality Act of 1995. As a trade organization representing over 700 manufacturers of health care devices, diagnostic products, and health information systems, HIMA has long taken a strong stand in support of privacy and confidentiality of medical records. We are encouraged that this area is now receiving the focus it deserves, but we are concerned that this bill does not consider a number of key points which must be addressed if the bill is to accomplish its key goals.

Increasingly we are functioning in an environment of electronic health care information support. HIMA looks forward to working with the sponsors to strengthen the bill so that the public and the health care industry can be better served. There are four areas of general concern our statement will address:

- **The purpose of the bill:** To limit access to patient records, and promote efficiency in the information infrastructure;

- **Practical considerations**
  -- *Paper vs. electronic records*;
  -- *Timeframe: one year is too restrictive;*

- **Distinctions between the types of privacy records**
  -- *Rights to the data;*
  -- *Validity of record actions*;

- **Definition and responsibilities of Health Care Trustees.**

Comments on specific provisions of the bill are also provided.

GENERAL COMMENTS

Purpose: Limit Access, Promote Efficiency

The purpose of developing the bill is to control inter-organizational access to health records which are personally identifiable, while promoting efficiency in the information infrastructure. Although access limitations are clearly necessary, the language is overreaching in the context of direct patient care activities within a single organizational setting. This may have the unintended effect of making record systems *less* efficient and actually jeopardize the quality of patient care.

We do not believe that the intention of this bill was to restrict the interchange of information among providers within a hospital, clinic, or other integrated health delivery system or network. It is clear that patient

care would suffer appreciably if an individual authorization were necessary every time a new physician, nurse, technician, or therapist were involved in the care of a patient. In general, the more timely patient care is, the higher the quality of such care. Conversely, putting barriers and impediments into the flow of direct patient care will raise costs and decrease quality.

Practical Considerations

Paper vs. Electronic Records

The status quo is often the starting point for any effort to change or strengthen a given practice or system. In this instance, the starting point is the paper record. However, the medium in use with growing frequency is the electronic medical record which has both advantages and limitations. In reforming the approach to medical record confidentiality, one must consider the distinctions between paper and electronic media.

Electronic records are superior to paper records in many ways, allowing information to be made available to providers rapidly and in a form in which it is most useful. However, there are fundamental differences between the two kinds of information. The appending of a "correction" and a refusal to each report as described by the bill is difficult enough if on paper. The appending of computer records to represent the various scenarios contemplated in the bill will become even more complex. In the context of the numerous industry-wide ongoing efforts toward standards development, such issues should be considered and integrated appropriately into the bill.

Short Timeframe for Implementation: One year is too restrictive

We believe the time allotted for promulgation of regulations and for implementation of the provisions -- 6 months and 12 months respectively -- is too agressive. The question becomes one of philosophy versus practice. Ideally, stronger restrictions on medical record confidentiality should be in place immediately. But, the patient protection provisions as described in S. 1360 have strong implications for providers, insurers, and manufacturers of health information systems alike. Such an undertaking should commence only with careful consideration of the burden placed on those entities that could lessen the benefits for patient care currently achieved through the automation of medical records.

In addition to improvements in patient care, tremendous economic benefits have been witnessed through use of the electronic medical record. At a time of severe budgetary constraints we should examine all aspects of the confidentiality requirements as they are developed so not to negate those savings already realized.

Distinctions Between Types of Records

An unusual blend of strict privacy protections and credit reporting protections have been woven into this bill. Unfortunately, such blending fails to consider the differences between health care information and consumer information. For example, almost all credit information is a direct derivative of actions of the consumer, but most health care information is not. The laboratory tests, the clinician's impressions of drug reactions, interpretations of information, reports on operative findings and other elements of the patient record represent information about a patient which is created by the provider, not by the patient. Taking this into account, two anomalies become clear from examination of the bill:

Who has rights to the data?

Is the data only the property of the patient, or does the provider also have rights to or in the data they have created? Under this bill, this issue is not addressed. It might be assumed, therefore, that providers have no rights in the data, despite the fact that such data generally represents their sole intellectual property. It is clear that the patient should have the right to access such data, and to provide for its distribution in a designated way. It is equally clear that the originator also needs standing.

The medical record represents not just an individual patient's record, but also a health care provider's primary business record. It is clear that to make this bill effective and useful, the rights of both patients and health care practitioners and information enterprises must be considered.

Whose reporting actions are considered valid and final?

Another problem emerges from the use of credit bureau standards for patient records. Because credit bureau records fundamentally rely on actions of a reportee, in general the individual involved has full and complete knowledge of whether the credit bureau record is correct or not. That is, if a bill was paid the individual has the canceled check.

In terms of health care information, in almost all cases, other than perhaps history, the patient does not have access to appropriate information to correct or amend such records. If the patient disagrees with the clinician's impressions, do the patient's impressions of the clinician's diagnostic acumen have standing? One would think not. If the patient has a lab test repeated a month later, and comes up with a different result, which lab test is correct?

Even if the result is different, it is likely that it was correct at the time the first test was done.

Yet, this bill allows a patient, even if their request for correction or edition is misguided or malicious, to force each clinician along the chain, as well as every information system to either make the correction, or to create a follow-on record disputing the patient's claim. Further, the follow-on record must include all reasoning, and then on the same point-by-point basis, forever follow the record. The magnitude of complexity that this will add to the system, for no practical benefit, has perhaps not been well considered. Other than demographic or historical information, for which the patient likely has independent information, some other mechanism must be created to address these kinds of issues.

Definition and Role of the Health Information Trustee

The role of Health Information Trustee is not clear. Any number of practitioners might be subsumed under a particular enterprise's definition of the Health Information Trustee. However, as described in S. 1360, a separate authorization could be required every time any new individual is involved in a patient's care. In light of the major effects this would have on the health care delivery system, this could not have been the intent of the legislation.

The management of medical information between or among entities is also unclear. Further, no distinction is drawn between physician and processor, although it might be implied by the language, there is no specific requirement that information disclosed by a Health Information Trustee to another Health Information Trustee or Health Information Service or to anyone else needs to continue to be managed in the way the originator manages the information. There should be a "chain of custody" such that at no point does protected information by neglect, or design become no longer subject to the rules set forth. Alternatively, secondary, non-originator Trustees should not be permitted to further disseminate protected information they have received.

SPECIFIC COMMENTS

Section 3, Definitions, (14) -- Protected Health Information

A "reasonable basis" test for something as compelling as the delineation between protected and unprotected health information has inadequate legislative support. There are too many combinations of demographics, identifiers, and encounters that one could construe as providing

identification. Considering that the entire success or failure of this approach depends on this delineation, more study should be accorded this key area.

Title I -- Individual's rights
Subtitle A -- Review of Protected Health Information by Subjects of the Information

Section 101 (b) (2), Confidential Source

This kind of language has enormous negative implications for information systems. This provision would require a confidential source designator to be appended to virtually every information system data item and/or data set, causing an enormous increase in overhead for the small number of occasions where actually needed.

Section 101 (b) (3) (A), Administrative Purposes

As noted above, the business records of a health care provider are virtually inseparable from the patient records. Health care delivery *is* the business of a health care provider. The delineations between patient and nonpatient information are blurred. Strictly constructed, it is likely that almost no information germane to the operation of a provider's business would be disclosable under this exception. This carve-out therefore needs specific definition. Similarly, the provision that disclosure is not required under the administrative provisions but only if it has not been disclosed to any other person is unclear. If it is administrative information, and the provider chooses to disclose it to one person and not to another, this would be well within the provider's purview.

Section 102 (a) (1), Correction or Amendment

As a general practice in all medical care, medical records may never be corrected. All corrections are handled as an amendment. This bill would imply that a new standard for such records was being contemplated. This might compromise the usefulness of medical records to track a patient's course of care, especially when erroneous data might have been acted upon. This should be clarified.

Section 102 (a) (3), Correction or Amendment

A specific definition of "reasonable effort to inform" must be provided legislatively. The burden to forward corrections and amendments in perpetuity to all persons receiving previous disclosures will become formidable. Again, major mechanisms will need to be put into place to handle a small number of cases. Compliance with this provision will likely

end up being excessively costly and/or impractical. Issues such as who pays for the cost of such retransmission of corrected information, time limits, etc., must be addressed.

Section 102 (c), Statement of Disagreement

Based on this clause, the Statement of Disagreement must be attached or linked to every potential data item entered or data set in dispute. As noted above, and because in almost all cases it is likely such disagreements will be disputed, a complete reworking of virtually all information systems would need to be accomplished. To achieve such linkages, for the small number of occasions where they are actually needed is overreaching. Further, all current standards will need to be fundamentally and extensively modified to include all such linkages for every possible data transmission.

Section 102 (e), Correction

See comments above with regard to Section 102 (a) (1). It appears under this subsection that information may simply be corrected, instead of generating an amendment to correct the record under current practice.

Subtitle B -- Establishment of Safeguards

Section 111 (b) (1) (S) (II), Advisory Group Membership

Conspicuously absent in the Advisory Group are representatives from health care information system developers, vendors, and informatics standards development organizations. Because these organizations must implement whatever is determined, their absence from the Advisory Group will likely compromise any end product.

Title II -- Restrictions on Use and Disclosure

Section 201 (b) (1), Compatibility to Purpose

This clause is overreaching, suggesting that all potential uses for health care information must be known and accounted for as a predicate for information capture. At least two other items need to be considered. First, as described in the General Comments above, those involved in the immediate and direct care of a patient should be exempt from such use requirements. Further, strict construction might preclude important uses which were not at first considered, such as quality assurance, nosocomial infection control, and other uses which may arise. In many of these cases, the identity of the patient is key.

Section 201 (d), Identification of Disclosed Information as Protected Information

To append a message to every computer screen and every inter-system interchange that says "protected data" will again create significant overhead and information technology issues. Millions of screens are interchanged among care providers continuously. To insist that every screen include an extra protected notice again seems overreaching. The solution of putting a one line notice on each screen soon becomes "invisible." Further, it removes screen space that could be better used for display of patient data.

Section 202, Authorizations for Disclosure of Protected Health Information for Treatment of Payment

Again, intra-organizational use is not separated from extra-organizational use. As noted in the General Comments, this creates an overwhelming impediment to the normal discourse and exchange of health care information in direct patient care. This is unnecessarily burdensome when imposed on health care practitioners working together as a team to provide care within a single enterprise. There must be a distinction between a health record maintained and used within an enterprise or network, and one that is transmitted externally.

Section 213, Standards for Electronic Disclosures

Standards for electronic disclosures are key in the protection of health care records going into the future. Greater specificity is needed in this area. Here is where information regarding intra-institutional contact, as well as practical extra-institutional contact should be developed.

Title III – Sanctions

Section 301, Civil Penalty

In an electronic age, it is possible for remote users (of which there will be many) to legitimately obtain records, and then to use them in an illegitimate fashion. This is no different than photocopying a piece of paper and doing something illegal with it. It is not clear, however, that the Trustee should be responsible for the illegal acts of each and every one of its employees and agents when such have been appropriately trained and have signed the appropriate statements saying they will not perform such illegal acts.

STATEMENT OF THE AMERICAN PSYCHIATRIC ASSOCIATION

The American Psychiatric Association (APA), a medical specialty society representing more than 42,000 psychiatric physicians nationwide, is pleased to present our recommendations to strengthen and improve the protection of the privacy of psychiatric treatment records as provided for in the Medical Records Confidentiality Act of 1995 (S. 1360).

We are deeply concerned that the legislation intended to address the critical issue of medical record privacy fails to meet the need for patient/psychiatrist confidentiality in the treatment of mental illness (including substance abuse). The bill is not a federal privacy law but instead establishes medical record disclosure guidelines. We appreciate that the authors of this legislation, Senator Robert Bennett, Chairman of the Senate Republican Health Care Task Force, and Senator Patrick Leahy, and the cosponsors are well intended with respect to limiting medical record disclosure. Regrettably, the bill creates a disclosure code for individually identifiable health information about a patient. It does not prohibit the release of a patient's medical record without patient consent. We find the bill's philosophy most troubling and creating a dangerous precedent.

It is not dissimilar to the Congressional Medicare promise. Thirty years ago the program was designed to protect the physician/patient relationship and the bill stated:

> Nothing in this title shall be construed to authorize any Federal officer or employee to exercise any supervision or control over the practice of medicine or the manner in which medical services are provided... 1

Need we remind the Committee that since that time, volumes of Medicare law have directly "controlled" the practice of medicine.

We are concerned that the Medical Records Confidentiality Act, despite any similar disclaimers respecting its discretionary nature and good intentions would, as it is currently drafted, successfully codify and legitimize release and transmission for profit of an individual person's medical record information without that patient's consent.

The APA strongly supports preserving medical record confidentiality and protecting the privacy and security of sensitive personal information. We understand it is necessary to draw a new balance between society's need to provide an ambience in which patients may be restored or helped to a state of maximum productivity and to provide access to information required by a complex society and its health care delivery system. While we exploit our advances in technology, we must be concerned where one's sole purpose is to enhance corporate technology profits, not patient care. We must uphold and protect a fundamental tenet of medicine: protecting the confidentiality of patient medical information critical to the patient's treatment.

Mental illnesses and substance abuse disorders do not discriminate by race, age, gender or ability. Today there are nearly 40 million adults in the United States who suffer from mental disorders or alcohol or other substance abuse.2 These 40 million Americans deserve to be treated with more than just dignity and respect; they are entitled to have their individual medical records kept confidential if we truly want them to enter into proven cost effective treatment.

During the extensive debate on reforming America's health care delivery system that took place in the 103rd Congress, proponents of a federal medical record confidentiality law repeatedly referred to a public opinion poll conducted by Louis Harris and Associates for Equifax, Inc. (Harris survey). "The poll found an overwhelming majority (eighty five percent) of the public believe that protecting the confidentiality of health records is absolutely essential or very important in national health care reform."3 While the eighty-five percent number is the oft cited statistic from the survey, the study provides other insights that, as Congress continues to debate confidentiality legislation, deserve attention.

The Harris survey indicated that users of mental health services, "score higher than non-users in their general privacy concerns and in favoring strong legal protections of medical privacy."4 The survey reported that these patients and family members, as a group, are more concerned than others regarding several issue areas, including:

- saying they did not seek medical treatment to avoid jeopardizing opportunities;
- paying bills to avoid submitting medical claims;
- worried about changing health insurance if they change jobs.5

According to the Harris survey, "Users of mental health services -- almost one in four members of the public plus additional members of their families who may have used such services -- clearly constitute one of the most high-concern segments of the public on issues involving the handling of sensitive medical information."6 Thus, of the 11% of those people surveyed who responded affirmatively when asked if they or an immediate family member had ever paid for a medical test, treatment, or counseling rather than submit a bill or claim under a health plan or program, it is likely that the most probable reason was the concern attached to the confidentiality of the mental health record.

Why do individuals who suffer from mental illnesses place such a high premium on protecting their medical records? To answer that question honestly, one must ask: why, when announcing that he would not run for President of the United States in 1996, did General Colin Powell have to answer a question regarding his wife Alma's depression? Why was Vincent Foster afraid to seek professional help for his condition? Why does the American public, sadly, find humor and entertainment value in psychiatric disorders and treatment? Stigma. Because of the stigma, rooted in fear and ignorance, psychiatric patients have legitimate reasons to seek assurances from their elected officials that the confidentiality of their medical records will be preserved.

The Medical Records Confidentiality Act of 1995, S. 1360, would establish a uniform federal code for disclosure of medical record information. Under the legislation, individuals would be permitted to inspect, copy and "correct" their medical record. The Secretary of Health and Human Services is directed to develop model written authorizations whereby the patient would be able to authorize release of medical record information. While the bill restricts the release of "protected health information" to, "use[s] or disclosure[s] compatible with and related to the purposes for which the information was obtained," S. 1360 outlines a variety of entities that may

receive medical record information from third party "Health Information Trustees" (trustees) without first obtaining patient consent. These include: Health Information Services (defined in the bill); Next of Kin; for Directory purposes; Emergency Circumstances; Oversight purposes; Public Health; Heath Research; Judicial and Administrative purposes; Law Enforcement; and Non-Law Enforcement Subpoenas. The bill also imposes criminal and civil penalties for violations of this act.

It is important to note that the legislation under consideration lists two of three purposes that, at first glance, may appear contradictory:

> (1) establish strong and effective mechanisms to protect the privacy of persons with respect to personally identifiable health care information that is created or maintained as part of health treatment, diagnosis, enrollment, payment, testing, or research process;
>
> (2) promote the efficiency and security of the health information infrastructure so that members of the health care community may more effectively exchange and transfer health information in a manner that will ensure the confidentiality of personally identifiable health information.

As noted earlier, the APA recognizes the need to strike a balance between society's need for and access to information, and the patients right to doctor/patient confidentiality. We underscore, however, that any legislation passed by Congress must not jeopardize the doctor/patient relationship. Not only does a physician bear a fiduciary duty to act in the best interest of his patient where these and other issues are concerned, but also, there is an expectation on the part of the patient that the physician will do exactly that. Often, regrettably because of stigma, the confidentiality of that relationship is the sine qua non for the patient entering into treatment.

Because the bill addresses issues of computerization through the promotion of efficiency and the transfer and exchange of health care information (more fully discussed below), and because many in Congress support computerization efforts not only to promote quality of care but also to combat health care fraud and abuse and reduce paperwork, it is appropriate to consider a risk benefit analysis of the computerization of the patient medical record. The Harris survey indicated that seventy-one percent of respondents agreed either strongly or somewhat that, "If privacy is to be preserved, the use of computers must be sharply restricted in the future."7 A recent episode of **60 Minutes** illustrated some of the problems associated with any information contained in a computerized system:

MIKE WALLACE, co-host: If you're going to cruise the information superhighway, like 30 million Americans are doing right now, you'd better be aware that cruising alongside you are intruders, hackers who can break into your computer and ferret out your credit records, your medical records, just about everything private that you wouldn't want to share with a stranger. . .Alan Brill heads up the worldwide high-tech security endeavors of Kroll Associates in New York.

Mr. ALAN BRILL (Kroll Associates): Everybody is telling you how great it is to get your company on the information superhighway.

WALLACE: Right.

Mr. BRILL: But they don't tell you that on this superhighway, there's carjackings, there's drive-by shootings and some of the rest stops are pretty dangerous places to hang around. Until companies understand that, they're putting themselves at risk...

WALLACE: How do the hackers break into a computer on the Internet? One of the easiest ways is by getting hold of the passwords that companies use, ostensibly to protect their computer files. But to demonstrate just how easy it is to uncover a password and break in, Alan Brill writes a brief message of his own.

'This is a corporate secret.'

Mr. BRILL: And I don't want anybody to see that message.

WALLACE: Right.

Mr. BRILL: Now if I tried to get that document, and if I don't know your password, the file is locked-not very good.

WALLACE: Right.

Mr. BRILL: There are programs that were developed for law enforcement. . .

WALLACE: Mm-hmm.

Mr. BRILL: . . .that, unfortunately, have kind of gotten out there. Guess where? On the Internet.

WALLACE: That program can pick out secret passwords because, when analyzed electronically, they stand out from the rest of the words in a file. Alan Brill was able to find my secret password within just seconds.

Mr. BRILL: The machine believes that your password was Zina.

WALLACE: There it is.

Mr. BRILL: With that password, I can get in and I can be you.

WALLACE: Which means he'd have access to all the files in my computer.8

Protecting the confidentiality of medical record disclosures is especially imperative for those who

need and obtain psychiatric treatment. The APA submits the following recommendations to strengthen S. 1360 and urges the committee to support the changes outlined below.

Section 3 includes definitions for Certified Health Information Services (CHIS) and Health Information Services (HIS). We understand that the HIS would facilitate the transfer of protected health information; as defined in the bill. The CHIS would be the entity responsible for "scrubbing" identifiers from medical records to produce non-identifiable health information. While we appreciate that, in fact, there are currently organizations that store and transmit medical record information in a computerized fashion, and that it is the intention of the authors to impose the duties of trustees (and penalties for violations) outlined in the bill, the APA strongly believes that the potential creation of a health information network threatens the doctor /patient relationship by jeopardizing, in a global fashion, the confidentiality of that relationship. No law passed can guarantee the protection of any item of value -- however, the World Wide Web and other technological advances we have achieved, have raised the stakes tremendously.

Federal legislation should not require patients and other participants in the health care system to transmit information electronically. The debate on the computerization of medical records is in and of itself worthy of public scrutiny. *The definitions of an HIS and CHIS in Sections 3 (1) and (6), the creation of non-identifiable information in Title II, Section 204, and the establishment of standards for electronic disclosure in Title II, Section 213 go beyond the scope of the bill and should be deleted.*

Federal legislation should not interfere with the medically necessary treatment of patients. Title I, Section 101 of S. 1360 provides for the inspection and copying of protected health information by the subjects of the records. The committee will be interested to know that in the Harris survey cited earlier in this statement, seventy-six percent of the individuals surveyed never asked to see their medical record. Of the twenty-four percent that did request to see their record, ninety two percent were either given their complete record or shown a complete copy; ninety

seven percent of those respondents thought they understood the information or had it explained to them in a satisfactory way.9 The fact of the matter is that very often, physicians, including psychiatrists, educate patients on what is in their records, particularly since patients are concerned about issues such as reimbursement and capitation of visits.

Inspection and copying of mental health treatment notes (as distinguished from what is commonly thought of as the "medical record" ie: diagnosis, charts, test results) by psychiatric patients may endanger the course of treatment and not be in the best interest of the patient's welfare. For example, a psychiatric patient suffering from Borderline Personality Disorder can not hold ambivalence in their mind simultaneously. These patients see the world and circumstances as black or white. While it could be eminently clear to the psychiatrist that the patient is suffering from this disorder, and mental health treatment notes may reflect this, it is quite possible that the patient would read this as a negative statement. One of the arts of psychotherapy is timing, and to impose a requirement on the psychiatrist to share with the patient understandings, interpretations, and thoughts of the practitioner, when the patient is not ready may not reach the "Endangerment to Life or Safety" standard outlined in the bill, but could very well endanger the therapy. A patient exposed to these notes at the wrong time might elect to discontinue treatment, and jeopardize their recovery. *Title I Section 101(b) should be amended to include a mental health treatment note exception which would prevent inspection or copying pursuant to the health professional's judgment that such inspection or copying would be detrimental to the patient's treatment and cause sufficient harm to the patient.*

Federal legislation should place a legal duty on <u>all</u> individuals and entities that create, collect, or use personally identifiable health information to protect the confidentiality of that information. Title I, Section 103 requires that Health Information Trustees, other than Health Information Services, shall provide in a clear and conspicuous manner, written notice of the trustee's information practices, including a description of the trustee's information practices. Patients are entitled to know who has their medical record, and what they are doing with it. *While the APA*

advocates striking all references to Health Information Services in the bill, at the very least Title I, Section 103 should be amended to strike the reference here.

S. 1360 would establish an Advisory Group to review all proposed rules and regulations and submit recommendations to the Secretary. The Secretary may also promulgate regulations in consultation with privacy, industry, and consumer groups. It is imperative that those concerned about mental illness, both physicians and patient communities, be included explicitly in these capacities. *"Physicians" should be added to Title I, Section 111(b)(1)(B)(I), and Section 111(b)(2) should also be amended to add "Physicians".*

Federal legislation should not permit the disclosure of confidential information that identifies an individual without the individual's consent except in narrowly-defined emergency circumstances. Title II, Sections 202 and 203 provide for the written authorization of disclosure of medical record information. Two distinct and dramatic problems present themselves under the bill as drafted. If a patient innocently, orally, requests that a physician convey protected health information as defined in the bill, and the physician does so, is he or she in violation of federal law? For example, if a patient is out on a lake fishing with his friend who is also his doctor, and another person, and the patient turns to the doctor and states, "tell my friend about that kidney problem I had last year," would this action violate the proposed law? The information is protected health information, thus, the patient could only release with a written consent.

Section 203(a)(3) prohibits providers from requesting that patients authorize the release of medical record information on a day on which the provider renders health care to the individual. The underlying rationale for this prohibition may be a concern that patients may be coerced into signing authorization forms when such forms are offered to them concurrent with the receipt of medical care. This concern seems farfetched, and the practical difficulties likely to be engendered by this prohibition are substantial.

For outpatients, facilities and providers will be unable to request previous treatment records unless the patient makes a special visit, on which no health care is rendered, in order to provide such authorization. Inpatients would be rendered ineligible to provide such authorization throughout their entire hospitalization. *We recommend that this section be deleted.*

S. 1360, Section 205 permits the disclosure of protected health information to the next-of-kin and for directory information. While the bill provides the patient with notice and an opportunity to object, there is a presumption that the information may be disclosed unless the patient objects; thus, the burden is on the patient to object. *Title II, Section 205 should be amended to reflect that the trustee shall not, unless consistent with legal and ethical medical practice, disclose protected health information unless the individual who is the subject of the information has been notified and concurs.*

The release of medical record information by third party "trustees" undermines the traditional doctor/patient confidential relationship. Taking the physician out of the information-disclosure process prevents the physician from notifying the patient of attempts to obtain private, personal medical records and informing the patient of potential consequences of disclosure. Even the Institute of Medicine report, Health Data in the Information Age: Use, Disclosure and Privacy, cited by proponents of computerization of medical records refers to the Workgroup on Electronic Data Interchange (WEDI) recommendation that, federal legislation include provisions that, "establish appropriate protections for highly sensitive data, such as data concerning mental health."10 While the APA supports Title IV's preemption exception for state mental health laws in Section 401(c)(3), we believe that it is appropriate for federal legislation to impose greater protections on psychiatric records. *S. 1360 should be amended to reflect that any records, including psychiatric records, pertaining to mental health treatment, may only be released by the health care professional in possession of the records or his/her designee.* Federal legislation should maintain current law and not allow law enforcement agencies to access confidential, personally identifiable medical information without a court order. *Title, Section 212 should be deleted.*

S. 1360 provides an exemption from liability for permissible disclosures made pursuant to the legislation in Section in Title IV Section 402. This is a particularly disturbing section of the proposed legislation in that it changes the current standard of care in the practice of medicine. For example, if a physician discloses protected health information to a third party as permitted in the bill, despite that fact that he or she may be in violation of professional practice standards, even if a jury were to find that the physician breached his or her fiduciary duty in revealing the information, the physician would not be held liable under the bill. Section 402, while intended to protect those parties who comply with the law in good faith, actually lowers the standard of care in medicine. Section 402 should be deleted.

Sensitive, private material should not be treated as a commodity -- to be indiscriminately bought and sold -- particularly by those motivated by corporate and marketplace profiteering and of questionable ethics. The creation of a health information network and network services that store protected health information will be of interest to both those with a legitimate concern for patient welfare and those whose only interest is abusive or destructive. As noted earlier throughout this statement, the APA strongly supports a fundamental rationale of protecting medical records. Federal legislation should protect personally identifiable information by ensuring that the following principles are contained in any legislation passed by Congress:

> Federal legislation should not undermine the traditional doctor/patient confidential relationship by taking the physician out of the information-disclosure process and, therefore, preventing the physician from notifying the patient of attempts to obtain private, personal medical information or to inform the patient of potential consequences of disclosure.
>
> Federal legislation should not permit the disclosure of confidential information that identifies an individual without the individual's consent except in narrowly-defined emergency circumstances and situations. Providers, patients, and other participants in the health care system should not be required to transmit information electronically.

Federal legislation should not preempt, supersede or modify state confidentiality, privacy, privilege or medical record disclosure statutes or federal or state common law findings that protect patient medical record information. Federal legislation should provide a "floor" of uniform protection for all personally identifiable medical record information; states should be allowed to provide stronger privacy protection for their citizens if needed.

Any interference with the maintenance of the confidentiality of psychiatrist/patient communications impairs the ability of a psychiatrist to help his or her patient. To the extent that such communications are disclosed without the patient's consent, the reliability of the physician/patient relationship is eroded, and the ability of a physician to help his or her patient is impaired. The APA urges the committee to accept what court after court has recognized as a legitimate zone of privacy--the psychiatrist/patient relationship--and protect the confidentiality of an individual's psychiatric medical records.

In closing, the American Psychiatric Association thanks the Committee for this opportunity to present our views on the Medical Records Confidentiality Act of 1995, S. 1360.

Notes:

1. Sec. 102(a) of the Social Security Act Amendments of 1965 (P.L. 89-97).

2. Health Care Reform for Americans with Severe Mental Illnesses: Report of the National Advisory Mental Health Council, produced in response to a request by the Senate Committee on Appropriations, *Am J Psychiatry 150:10*, October 1993 ("mental disorders" refers to conditions that impair life's major functions, not brief periods of anxiety, panic or low spirits that people commonly experience).

3. House Comm. on Government Operations, H.R. Rep. No. 103-601 Part 5, 103D Cong., 2d Sess. (1994) (report to accompany H.R.3600).

4. Harris-Equifax *Health Information Privacy Survey 1993*, Louis Harris and Associates, New York, New York, p.12.

5. Id.

6. Id.

7. Id. at Appendix B card 1 p. 1

8. 60 Minutes CBS News, Feb. 26, 1995, Volume XXVII, Num. 25, Burrelle's Information Services, Livingston, New Jersey.

9. Harris at Appendix B card 1 p. 3.

10. *Health Data in the Information Age: Use, Disclosure, and Privacy*, Institute of Medicine, 1994, p. 181.

[Whereupon, at 12 p.m., the committee was adjourned.]

o