CONFIDENTIALITY OF PATIENT RECORDS

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

FEBRUARY 17, 2000

Serial 106–89

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
66–897 CC WASHINGTON : 2001

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

COMMITTEE ON WAYS AND MEANS

BILL ARCHER, Texas, *Chairman*

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

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

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

SUBCOMMITTEE ON HEALTH

BILL THOMAS, California, *Chairman*

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

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

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

CONTENTS

CONFIDENTIALITY OF PATIENT RECORDS

THURSDAY, FEBRUARY 17, 2000

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

The Subcommittee met, pursuant to notice, at 11:37 a.m., in room 1100, Longworth House Office Building, Hon. Bill Thomas (Chairman of the Subcommittee) presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON HEALTH

FOR IMMEDIATE RELEASE CONTACT: (202) 225–3943
February 11, 2000
No. HL–13

Thomas Announces Hearing on the Confidentiality of Patient Records

Congressman Bill Thomas (R–CA), Chairman, Subcommittee on Health of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing on the Administration's proposed regulations regarding privacy of individually identifiable health information. The hearing will take place on Thursday, February 17, 2000, in the main Committee hearing room, 1100 Longworth House Office Building, beginning at 10:00 a.m.

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. The Subcommittee will receive testimony from a representative of the U.S. Department of Health and Human Services (HHS), and from a variety of private sector witnesses representing different perspectives from within the health care system. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

BACKGROUND:

Congress addressed the issue of medical record confidentiality in 1996 when it passed administrative simplification requirements for electronic health transactions as part of the Health Insurance Portability and Accountability Act (HIPAA) P.L. 104–191). HIPAA required the Secretary of HHS to make recommendations to Congress about how to better protect the confidentiality of personal health information that is transmitted electronically. The Secretary submitted her recommendations to Congress in September of 1997. Additionally, Congress granted the Secretary the authority to draft regulations if a privacy law was not enacted by August 21, 1999. On November 3, 1999, HHS published a Notice of Proposed Rule Making for ''Standards for Privacy of Individually Identifiable Health Information.'' The comment period for this ruling was extended until February 17, 2000, and a final ruling will follow. Generally, covered entities must comply with these regulations no later than 24 months following the effective date of the final rule.

The proposed rule establishes standards to protect the privacy of individually identifiable health information maintained or transmitted electronically in connection with one of the mandated electronic transaction standards established by HIPAA. Since the release of the proposed ruling, many provider groups, health care organizations, and privacy advocates have expressed various concerns about different interpretations of the regulation, and its potential implications. As a result, thousands of comments are expected to be submitted on the regulation by the end of the comment period.

In announcing the hearing, Chairman Thomas stated: ''Protecting the confidentiality of personal health information is critical to ensuring patient confidence in our health care system. The Secretary has taken on a monumental task. She has tried to lay out a comprehensive framework for regulating the flow of virtually all health care information, while still allowing data to be used to further research that will improve patient care. This hearing is intended to assist us in determining whether

the regulation will ultimately prove to be workable or whether legislation might be necessary."

FOCUS OF THE HEARING:

The hearing will focus on various aspects of the Department's proposed confidentiality regulation, and examine what implications the rule presents for Medicare and the private health sector.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Any person or organization wishing to submit a written statement for the printed record of the hearing should submit six (6) single-spaced copies of their statement, along with an IBM compatible 3.5-inch diskette in WordPerfect or MS Word format, with their name, address, and hearing date noted on a label, by the close of business, Thursday, March 2, 2000, to A.L. Singleton, Chief of Staff, Committee on Ways and Means, U.S. House of Representatives, 1102 Longworth House Office Building, Washington, D.C. 20515. If those filing written statements wish to have their statements distributed to the press and interested public at the hearing, they may deliver 200 additional copies for this purpose to the Subcommittee on Health office, room 1136 Longworth House Office Building, by close of business the day before the hearing.

FORMATTING REQUIREMENTS:

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

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

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

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

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

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

Note: All Committee advisories and news releases are available on the World Wide Web at "http://waysandmeans.house.gov".

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

Chairman THOMAS. The subcommittee will come to order. When I was younger there was a little rhyme that my mother used to recite to me and I never really appreciated it as much as I do now when the House is not going to meet and vote today, and members make choices. We had planned on voting today. We will not have as many members at this hearing as we obviously would like. There are others that are forced to arrive a little late because of other factors.

But the little rhyme was that man works from sun to sun, a woman's work is never done. This committee has a decidedly female bent in terms of the workload that we have. But we are dealing with a number of issues in which we need to lay a hearing record fairly early, and frankly, I believe February is a fairly early time period, in looking at issues such as medical errors, prescription drug being integrated into Medicare.

Nothing is probably more important since it undergirds many of those areas, the question of medical records, confidentiality of those records. But more importantly, the ability to use those records in a confidential way to continue to work on a systematic examination of medical decisions for outcomes policy and for making sure that with the limited dollars available, to try to stretch as far as we can to provide health care to a number of individuals in our society, among those the eldest and the most needy, the taxpayers' dollars are spent in the wisest possible way.

Congress addressed the issue of medical record confidentiality in 1966, although the whole question of confidentiality in the general area of records has been looked at since the 1970s. In the legislation, the Health Insurance Portability and Accountability Act, there was a positive attempt to get at especially the area of electronic health transactions. We had a deadline for Congress to act, but with some degree of prescience said that if we did not, the Secretary of Health and Human Services should go forward with the attempt.

The context in which we examine the Secretary's attempt, and indeed look at Congressional attempts, one to meet the deadline, and continue to try to produce policy after the deadline even today, is one that I think has been an honest effort to deal with a very difficult area. There are some I think who would like to politicize this area as they are attempting to politicize other areas, and use it for whatever political advantage they may think.

As far as serving the society in the areas, for example, that we have held committee hearings on and this one today, I hope that we will try to tone down the politics. That is, the assumption that people who are in opposition to some attempt to create confidentiality in some manner have ulterior motives.

I think when you look at it from the number of different perspectives that people look at it, they all see the problem from a slightly different perspective and try to examine it from how they fit into the proposed scheme. Indeed, I am hopeful that with the initial panel of Health Care Financing Administration and the other panels it will be clearly illustrated that to a very great extent beauty

is in the eye of the beholder, depending upon how you see yourself within this larger structure.

So we come today with the last day of the extended comment period closing, and that is one of the reasons I wanted to make sure that we had a hearing today. Now generally, covered entities must comply with these regulations no later than 24 months following the effective date of the final rule. As we have seen with other legislation, that may be forever. Our goal is not to have that happen. To the degree regulations that seem to be generally supported cannot be finalized, then obviously legislation is even more critical.

So let me just preface our discussion by stating that the Secretary has undertaken a monumental task. I strongly support the overall goals of her proposal. Within the confines of the health care legislation the Secretary has tried to lay out a comprehensive framework while still allowing the data to be used for research, quality improvement, case and disease management, and other important purposes that sometimes we fail to realize how important they are until someone in one particular niche comes to us and says, you did not think about me. You did not realize that we do these sorts of things.

So this hearing is intended to assist us in determining whether the regulation will ultimately prove to be workable or whether, as I said, we really need to have legislation notwithstanding the best efforts. Obviously from the number of words on pages with this proposed ruling it is evident this is a complicated issue. From all indications, and I think we have got—hopefully in the testimony we will get some indication of the number of public comments. Since this is nearing the last day you may get additional, but you should have a pretty good idea of the count.

Frankly, this is helpful, useful. This kind of scrutiny is good. This is a very important area that we get right. Everyone agrees that patient records should be kept confidential. The difficulties come in determining the best way to accomplish that goal. How much, to what degree, in what instance, how clear is it? To me, the importance of this issue in health policy cannot be overstated. In fact it undergirds our attempts, especially in areas such as medical errors, to get it right.

So what we really need to do is listen carefully to all of the concerns, and indeed some of the difficulties of the Secretary in trying to put together a package, so that in our effort to maintain confidentiality we minimally hinder, if at all, the flow of information that is essential to the delivery of quality health care and improving the quality of care for patients in the future.

The Secretary's effort represents the Administration's initial attempt after several false starts at resolving this very perplexing policy challenge. Today begins this committee's examination of whether or not the effort is minimally acceptable or whether we are going to have to enter the legislative thicket in dealing with that.

[The opening statement follows:]

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

Good morning and welcome. Congress addressed the issue of medical record confidentiality in 1996 when it passed administrative simplification requirements for

electronic health transactions. This legislation, the Health Insurance Portability and Accountability Act (or HIPAA), required the Secretary of Health and Human Services to make recommendations to Congress on how to better protect the confidentiality of personal health information that is transmitted electronically. The Secretary submitted her recommendations to us in September of 1997. Additionally, Congress granted the Secretary the authority to draft regulations if a confidentiality law was not enacted by August 21, 1999. On November 3, 1999, Health and Human Services published their proposed regulations for medical record confidentiality. The comment period for this ruling was extended, upon our urging, until today, February 17, 2000, and a final ruling will follow. Generally, covered entities must comply with these regulations no later than 24 months following the effective date of the final rule.

Let me just preface our discussion by stating that the Secretary has undertaken a monumental task and I strongly support the overall goals of her proposal. She has tried to lay out a comprehensive framework for regulating the flow of health care information, while still allowing data to be used for research, quality improvement, case and disease management, and other important purposes that will improve patient care. Today the Subcommittee will be examining these proposed regulations and the possible effects that they may have on the health care system. This hearing is intended to assist us in determining whether the regulation will ultimately prove to be workable or whether additional legislation might be necessary. From the length of the proposed ruling, it is quite evident that this is a complicated issue. From all indications, HHS will have received a deluge of public comments by the end of today regarding this issue. This kind of scrutiny is good. For this rule will have broad implications. One thing is clear, we need to get this one right. Everyone agrees that patient records should be kept confidential, the difficulties come in determining the best way to accomplish this goal.

To me, the importance of this issue in health policy cannot be overstated. It is imperative that we ensure the confidentiality of Medicare beneficiaries' health information. Protecting the confidentiality of this information is critical to ensuring patient confidence in our health care system. Yet, it is equally important that, in the effort to maintain confidentiality, we do not hinder the flow of information that is essential to the delivery of quality health care, and to improving the quality of care for patients in the future. The Secretary's regulation represents the Administration's initial attempt at resolving this perplexing policy challenge. My hope is that today's hearing will be instrumental in helping us determine whether this initial attempt strikes the right balance.

With that I would yield to my colleague from Washington, someone who has a significant interest in this area and has attempted on his own in the past to help resolve the difficulties in this area. The gentleman from Washington, Mr. McDermott.

Mr. MCDERMOTT. Thank you, Mr. Chairman. I want to comment you on having this hearing, and I think that as you rightly state it is not a partisan issue. It is an issue of extreme importance I think for the health care system in this country. For that reason I think that it is important that we start as early in the session as we come airing the issues so that if we are going to write legislation in this session we ought to have an opportunity to actually let the public be involved in the process.

I practiced as a psychiatrist for about 20 years so privacy and patient's confidence that what he or she said to me would remain private has always been a crucial component of my personal practice, but it is in all of medicine. It is the basis for going to a doctor and saying to a doctor what my problem is. If you do not trust the physician, or the nurse or whoever the health provider is that this information is going to be kept private, you are liable to withhold or tell only half the story or whatever. So it is important if you are going to get good health care that you have privacy guaranteed.

But it is more than as an observer of standard medical practice that I became convinced we need strong Federal privacy laws. Having had surgery I have had already the impacts of getting a medication and then getting mailings from people that I did not know where they came from. I do not know who let these companies know that I was on a particular medication and therefore should send me medical device information. It is everywhere and everybody is being impacted on it, including members of Congress. This is not something that is Democrats or Republicans. It is everybody in this country who receives health care is a part of this system.

Now Congress had, as the chairman rightly says, a chance to establish standards but up to this point we have not done it. So I would like to commend the Administration, especially Secretary Shalala, for doing what the Congress so far has been unable to do and moving forward with the medical confidentiality standards. I want to thank the Secretary and the department for working within the constraints placed upon them by the Congress and delivering a good regulation.

Based on the thousands of comments—I understand the figure is in excess of 30,000 or 40,000—HHS has been receiving on this issue it is safe to say that they must be on the right trace, because they are coming from both sides or—there really is more than two sides. There are about nine sides to this issue.

But in spite of the good faith efforts by the Administration I think we all receive that adequate systemic protection of medical privacy cannot be achieved simply by regulation. When Congress passed the Health Insurance Portability and Accountability Act, the so-called HIPAA, Congress gave itself two years to do this. And if we did not act we said Donna Shalala, the Secretary, should do it. But we imposed severe restrictions—and I want to emphasize that—on the Secretary. These constraints are reflected by the narrow scope of the regulation that we have before us. In my view it is a narrow scope.

As members of the committee and as the Congress begins to think about this I think we have to keep in mind that we prevented the Secretary from doing more than is in this regulation. The only entities that are directly covered by the regulation are health care providers, health care plans, and health data clearinghouses. Additionally, the regulation only applies to electronic records.

Now I am the only one on the dais that ever filled out a health care record, kept records. Most of it is written, or has been for a very long time. The advent of the computer has changed it obviously, but for the regulation only to deal with electronic data seems to me an unnecessary or an improper narrowing of the scope of the regulation.

In addition, we also said there was a limited enforcement mechanism and no right to sue. If your information is used against you and you are unable to—if you are damaged in some way or feel you are, you have no right to go to the courts.

Now by restricting the entities covered by the regulation we left a huge vacuum of unregulated entities. For instance, researchers and oversight agencies that collect, use, and disclose protected health information will not be directly covered. Clearly, the only

way to ensure that all parties to sensitive health information are required to maintain privacy is through strong and comprehensive legislation. That is why I think the chairman is correct in holding this hearing and setting us on the road.

Now I started in 1995 on this issue after I read an article in the New York Times Sunday magazine section about a young man who had a disease called Marie-Tooth disease. It is a very rare upper limb muscular dystrophy which makes weak upper arms. He was taken and they did the genetic testing on him and all of this, and they did the counseling with the family.

The family thought that was the end of it until about three months later the father lost his auto insurance. Now he lost his auto insurance without a moving violation, with an accident. Just got a notice, you no longer are covered by our company. He started to investigate this and they told him that they had discovered that his son's disease was a genetic disease and they did not want anybody who had that disease to have their automobile insurance.

Now you ask yourself, how did that get from the doctor's office to the auto insurance company that pulled his policy? It is because we are all open to this, the entire public at this point can be affected by that thing. And I hope that the chairman will be willing to work with members of the entire committee on this issue. I think we have started well and I think it is a good thing to do because this is an issue that affects everyone. It is not going to get better. It is going to get worse as we go down the road.

It is increasingly difficult to ensure the privacy of sensitive health information because of the tremendous technological advances and the more efficient transmittal of large quantities of data. Computers have absolutely revolutionized the way medical information is collected, stored, and disseminated. If you walk through a hospital, doctors have computers in their lap and they are typing things into them and then dumping them into the larger mainframe and away it goes. So without adequate, enforceable controls, this information can easily be used to breach the privacy of patients and to allow discrimination against them.

Now rightly, Americans are becoming increasingly concerned about this lack of privacy. If we do not step in with strong protections we will seriously undermine the credibility of the health care system. That is, the doctor-patient relationship which we say we want to protect. But there is another issue which I want to put on the table and I think in some ways this hearing is really a precursor for a much bigger problem down the road.

The United States Government has spent billions of dollars in something called the human genome project. Soon we will have a map of the entire genetic makeup of the body. But while this scientific advance carries with it many promising benefits, it also raises significant concerns about privacy.

One test can determine a woman's potential susceptibility to breast cancer. The work was done at the University of Washington by a Dr. Mary Claire King and I know intimately what went on in that whole thing. But many in this country are unwilling to be tested because they are fearful that if it gets into their record that they have the gene, or it is in their record and their children are also receiving treatment or need treatment or are wondering about

it, they may lose insurance. The fear about having that genetic information known and in the computer system is a restraint on the kinds of prevention that would be possible if we had good assurance of privacy.

So we must ensure that our citizens can take advantage of medical breakthroughs without the worry that information may be used against them.

To I think we will also hear concerns from companies. Some of the information that I read comes from companies that make money from marketing of sensitive health information. But I believe medical records must not be commodities that are bought and sold. I think we may hear many claims that the new regulation must not interfere with those particular interests, but the group we have to listen to most carefully in my view are the patients and their families. Think about your own family records being available for anyone to look at and you immediately see what the problem is.

Now the question we have to ask ourselves as we write legislation is, what value can you place on the confidentiality of a doctor-patient relationship? It is essential that we protect the privacy of individuals, including their genetic privacy. Good legislation can ensure that the new technologies are used not to deny care or to deny medical privacy, but to benefit all of us.

Mr. Chairman, as I close I would like to enter in the record the following statements, one from Congresswoman Louise Slaughter, one from the American Psychiatric Association, one from the American Psychoanalytic Association, one from AFSME, one from the Consortium for Citizens for Disabilities, and one from the National Breast Cancer Coalition, and finally I would like attached a letter signed by a number of members of the Congress who are interested in this whole issue. This is a beginning of what I think is a very important process and I commend you on it.

Chairman THOMAS. Without objection, those will be submitted for the record.

[The opening statement and material follow:]

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

want to thank Chairman Thomas and the ranking member, Mr. Stark, for yielding me time to talk about medical privacy, an issue that I have been concerned about for some time.

Most of you know that I was a practicing psychiatrist for more than 30 years. Privacy, and the patient's confidence that what he or she says will remain private, is a crucial component of that profession. But more than that, as an observer of standard medical practices, I became convinced that we need a strong federal privacy law protecting patients.

Congress had a chance to establish those standards but couldn't do it. So I would like to commend the Administration, especially Secretary Shalala, for doing what the Congress hasn't been able to do and moving forward with medical confidentiality standards.

I thank the Secretary and the Department for working within the constraints placed on them by Congress and delivering a good regulation. Based on the thousands of comments HHS is receiving from all sides of the issue, it is safe to say they are on the right track.

But despite those good-faith efforts by the administration, I think we all realize that adequate, systemic protection of medical privacy cannot be achieved through regulation.

When Congress passed The Health Insurance Portability and Accountability Act (HIPAA), Congress gave itself two years to write comprehensive privacy regulations. If we did not act—and we didn't—then Secretary Shalala could issue rules. But we imposed some strict constraints on the secretary. These constraints are reflected by the narrow scope of the regulation before us.

As the members of the subcommittee listen to the testimony today, I urge you to keep in mind what we prevented the Secretary from doing. The only entities that are directly covered by the regulation are health care providers, health plans, and health data clearinghouses. Additionally, the regulation only applies to electronic records—not even paper records are protected—and there is a limited enforcement mechanism, and no right to sue.

By restricting the entities covered by the regulation, we have left a large vacuum of unregulated entities. For instance, researchers and oversight agencies that collect, use, and disclose protected health information will not be directly covered.

I applaud the Secretary's effort to limit disclosures by binding the business partners of cover entities through contracts. This intermediary step heads in the right direction by ensuring the rights of patients are not violated. Unfortunately, it targets the liability on covered entities, while failing to prevent re-disclosures by entities that are not covered.

The intent of HIPAA's Administrative Simplification section was to move the health care industry toward using electronic records—a worthwhile goal.

Clearly, we must take action to apply the regulation's protections to all patient records. Congress' preventing Secretary Shalala from covering paper records doesn't pass the laugh test. I believe the Secretary has the authority to cover both paper and electronic records and encourage her to do so in the final rule. Applying this regulation only to electronic records will create a disincentive for organizations to convert existing records to electronic form—which is contrary to Congress' intent.

Congress also failed to allow the Secretary to include adequate enforcement of the regulation. The enforcement mechanisms in this regulation are minimal at best. We have established rules for the use and disclosure of sensitive health information without providing meaningful repercussions for breaking them. Compounding the problem is the fact that Congress did not provide a right-to-sue provision in HIPAA.

Clearly, the only way to ensure that all parties to sensitive health information are required to maintain privacy is through strong, comprehensive legislation. In May 1996, I introduced my first medical privacy bill. I hope the Chairman will be willing to work with all members of the committee in pursuit of a strong, comprehensive, and bipartisan bill.

If privacy is not maintained, the public will lack confidence in our health care system. If individuals doubt their information will be kept private, they will either delay treatment or be less forthcoming with their physicians. This self-monitoring of personal health information will result in increased personal and financial costs. We could even see a decline in societal health stemming from the increase in transmission of communicable diseases.

Also, it is increasingly difficult to ensure the privacy of sensitive health information. Tremendous technological advances make it easier and more efficient to transmit large quantities of data. Computers have revolutionized the way medical information is collected, stored, and disseminated. Without adequate, enforceable controls, this information can easily be used to breach the privacy of patients and to allow discrimination against them.

Americans are becoming increasingly concerned about their lack of privacy. If we don't step in with strong protections, we will seriously undermine the credibility of our health care system.

One technological advance which we need to address is the Human Genome Project. Soon, we will have a map of the entire genetic makeup of the body. But while this scientific advance carries with it many promising benefits, it also raises significant concerns about privacy.

One test can determine a woman's potential susceptibility to breast cancer. But some women, afraid that they or even their daughters will be denied employment or health insurance if they carry the gene, won't submit to the test.

We must ensure that our citizens can take advantage of medical breakthroughs without the worry that private information may be used against them.

Today, we will hear concerns about companies that stand to make money marketing sensitive medical information. But, medical records must not be commodities that are bought and sold.

We may hear many claims that any new legislation must not interfere with those particular interests. But the group we should listen to most will be hardest to hear: patients and their families. Think about your own family's medical records being available for anyone to look at. What value can we place on the confidentiality of

the doctor-patient relationship? It is essential that we protect the privacy of individuals, including their genetic privacy. Good legislation can ensure that new technologies are used, not to deny health care or to deny medical privacy, but to benefit all of us.

Mr. Chairman, I would like to enter the following statements into the record:

1. Congresswoman Louise Slaughter;
2. American Psychiatric Association;
3. American Psychoanalytic Association;
4. AFSME, the American Federation of State, County and Municipal Employees;
5. Consortium of Citizens for Disabilities;
6. National Breast Cancer Coalition; and
7. The attached comment letter signed by a number of Democratic members of Congress who are leading health privacy advocates.

Thank you.

Chairman THOMAS. Now Dr. Hamburg, thank you very much for coming before us. Dr. Hamburg is the assistant secretary for planning and evaluation, U.S. Department of Health and Human Services. She is narrowly responsible, but obviously the Secretary is broadly responsible. And as is the case in our offices many times, we may be the point person but we are not the one that either has a broader command of the particular area, and Dr. Hamburg has asked Mr. Claxton to sit at the table. Since our goal is to try to understand rather than play gotcha, we are more than willing to allow that to occur.

So Dr. Hamburg, your written testimony will be made a part of the record and you can address us in any way you see fit in the time that you have available.

STATEMENT OF HON. MARGARET A. HAMBURG, M.D., ASSISTANT SECRETARY FOR PLANNING AND EVALUATION, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES; ACCOMPANIED BY GARY CLAXTON, DEPUTY ASSISTANT SECRETARY FOR HEALTH POLICY

Dr. HAMBURG. Thank you very much, Mr. Chairman, and distinguished members of the subcommittee. I appreciate the opportunity to appear before you to discuss the need for Federal legislation to safeguard the privacy of health information. As you know, health information privacy is the top priority for the department and the Administration and we continue to believe that legislation is the only way to achieve that goal.

I am joined by Mr. Gary Claxton, the deputy assistant secretary for health policy in my office who has been deeply involved with issues of health privacy and the development of the proposed reg.

At the outset, I want to commend the members of the subcommittee for their interest in health care privacy and efforts to develop this important and complex legislation. In addition, we are encouraged by the recent appointment of two Congressional task forces to address privacy issues. These efforts have the potential to generate the momentum needed to enact legislation this year.

We are here today to emphasize our support for passage of bipartisan legislation providing comprehensive privacy protection to people's health care information. Stories abound that raise concern that our sensitive medical information can enter the wrong hands and be misused. Almost 75 percent of our citizens say that they are

at least somewhat concerned that computerized medical records will have a negative effect on their privacy.

Numerous analyses by Government, industry, and professional groups have identified serious gaps in protections for health information and have recommended Federal legislation to close them. And of course, we have already heard your personal stories about this concern. If we do not act now, public distress could deepen and ultimately stop citizens from disclosing important information to their doctors or getting needed treatment.

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

The Secretary legislation to implement five key principles. First, information about a consumer that is obtained for delivering and paying for health care should, with very few exceptions, be used and disclosed for health purposes and health purposes only.

Second, those who legally receive health information should be required to take reasonable steps to safeguard it.

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

Fourth, people who violate the confidentiality of our personal health information should be accountable.

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

To prepare the proposed privacy regulation we assembled a team from all the relevant Federal agencies. We published the proposed rule on November 3rd, 1999 and the period for public comment, as you noted, closes today. We explained the basis for our proposals in detail in the preamble to the proposed rule, but also asked for comment on over 150 specific issues. We will review all the comments we receive and we will make whatever changes are appropriate.

We are committed to achieving the proper balance between ensuring patient privacy and the needs of the health care system to function properly and to continue advances in health protection and medical treatment. Our commitment to getting it right led us to extend the comment period from January 3rd to February 17th so the public and stakeholders would have adequate time to consider the proposed rule.

Since we have just begun to review the comments I will not be able to speculate on or debate the contents of the final rule today. But I can tell you that as of yesterday we had received about 40,000 comments by mail or hand-delivery and roughly another

10,000 on our web site. Further, we have met with dozens of individuals and groups to hear more about their concerns and clarify provision of the proposed rule.

While we are moving ahead to prepare the final regulation let me give you a few reasons why we continue to call for legislation. First, the HIPAA limits the application of our proposed rule to three entities, health plans, clearinghouses, and certain providers. But it does not provide authority for the rule to reach many people who receive health information from these entities. In short, in the rule we cannot put in place appropriate restrictions on how such recipients of protected health information may use and redisclose that information.

Second, we are concerned that the enforcement provisions in the HIPAA are not adequate. The penalty structure is not commensurate with the importance of privacy in our lives, and there is no statutory authority for a private right of action for individuals to enforce their privacy rights.

There are additional reasons we continue to call for legislation. For example, under the HIPAA only those providers engaged in electronic transactions can be covered. Any provider who maintains a solely paper information system cannot be subject to these privacy standards.

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

Thank you again for giving me this opportunity to testify and I look forward to answering any questions that you may have and working closely with you as you move forward on this important agenda.

[The prepared statement follows:]

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

Mr. Chairman, Congressman Stark, distinguished members of the Committee: I appreciate the opportunity to appear before you to discuss the need for federal legislation to ensure comprehensive privacy safeguards for health information. This issue is a top priority for the Department and the Administration, and although the regulation that we recently proposed serves as a foundation for providing strong privacy protections for consumers' health information, we continue to believe that legislation is ultimately necessary if we are to appropriately protect the privacy of the health information of all Americans.

As the outset, I want to commend the members of this Subcommittee Mr. Thomas, Mr. Stark, and Mr. McDermott, as well as Mr. Cardin, for their interest in health care privacy and efforts to develop this important and complex legislation. In addition, we are encouraged by the recent appointment of two congressional task forces to address privacy issues. The "Congressional Privacy Caucus" has the potential to generate the momentum needed to enact legislation this year.

As you may remember, Secretary Shalala first presented her recommendations, required by the Congress under Section 264 of the Heath Insurance Portability and Accountability Act (HIPAA), in September 1997.[1] I think it is fair to say that the

[1] Confidentiality of Individually-Identifiable Health Information, Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Port-

Continued

recommendations were well received and have been used to assist others in crafting their own legislative proposals.

HIPAA also requires that if legislation establishing comprehensive privacy protection was not enacted by August of last year, HHS must prepare final regulations. We assembled an interagency team to assist us in preparing the proposed regulation, including representatives from the Departments of Labor, Defense, Justice, Commerce, the Social Security Administration, the Office of Personnel Management, the Department of Veterans Affairs, and the Office of Management and Budget. We published the proposed rule on November 3 of 1999; the period for public comment closes today, February 17, 2000, and we will call upon a similarly broad team to review and respond to the public comments.

We explained the basis for our proposals in detail in the preamble to the proposed rule and asked for comments on over 150 specific issues. We are committed to reviewing all the public comments. Nothing in our proposed rule is set in stone. We are committed to achieving the proper balance between ensuring patient privacy and the needs of the health care system to function properly and continue advances in medical treatment. Our commitment to 'getting it right' led us to extend the comment period fro January 3 to February 17, so the public and stakeholders would have adequate time to consider the proposed rule, comment, and suggest alternative proposals.

Since we have just begun to review the comments, I will not speculate on or debate the contents of the final rule today. I can tell you that, as of yesterday, we had received over 30,000 comments by mail or hand delivery, and another 10,000 on our web site. Further, we met with dozens of individuals and organizations to hear more about their concerns and clarify provision of the proposed rule.

While we are moving ahead to prepare the final regulation, the President and Secretary Shalala have made it very clear that their first priority is to see Congress enact a health information privacy bill that builds upon the progress made by our proposed regulation and ensures comprehensive privacy protections. We believe our rule will be a very good start in providing confidentiality protections, but legislation is needed to complete this important task and provide the protections envisioned in the Secretary's recommendations. Our staff have been working closely with many of your staff, and staff in the Senate, to assist you in achieving that goal. Again, let me reiterate, we want to see legislation, and we want to work with you to make that happen.

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

THE NEED FOR LEGISLATION

It has been over 25 years since a public advisory committee appointed by former HEW Secretary Elliot Richardson set forth principles of fair information practices that led to the landmark Federal Privacy Act. The Privacy Act is premised on the idea that individuals have a right to know what personal information the government holds about them, how that information will be used, and the right to review that information. Those 25 years have brought vast changes in our health care system.

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

In addition, new discoveries in biology mean that a whole new world of medical tests have the potential to help prevent disease. However, they also reveal the most personal health information about an individual and his or her family. Without safeguards to assure citizens that getting tested will not endanger their families' privacy or health insurance, we could endanger one of the most promising areas of research our nation has ever seen.

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

Currently, when we give a physician or health insurance company precious health information, the level of protection will vary widely from state to state. We have

---

ability and Accountability Act of 1996" can be found on the HHS web site at: http://aspe.os.dhhs.gov/admnsimp.

no comprehensive federal health information privacy standards. Because the practice of health care is increasingly becoming interstate through mergers, complex contractual relationships and enhanced telecommunications, we can no longer rely on the existing patchwork of state laws. The patchwork does not provide Americans the privacy protections they need or expect. The Congress should seize upon this opportunity to create strong federal standards and reassure the public that they can trust their health care providers and insurers to keep their health information secure.

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

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

THE PRINCIPLES

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

Boundaries

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

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

We recommend that the legislation apply specifically to providers and payers, and to anyone who receives health information from a provider or payer, either with the authorization of the patient or as authorized explicitly by legislation. To the extent allowed under the HIPAA statute, we have taken this approach in our proposed regulation. Our proposed rule would authorize the use and disclosure of personal information by heath plans and providers without the person's consent for specified health care and national priority purposes, and would require fair and informed consent from individuals for all other uses. However, as discussed below, the statute limits our authority to ensure that information that leaves a health plan or provider remains protected.

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

The numbers and types of service organizations are increasing every day. While most do not have direct relationships with the patients, they do have access to their personal health care information. Therefore, we recommend that they should be bound by the same standards. For example, a health plan's contractor should be allowed to have access to patient lists in order to do mailings to remind patients to schedule appointments for preventive care. But it should not be able to sell the patient lists to a pharmaceutical company for a direct mailing announcing a new product (without the person's consent). With the Business Partner provisions of our proposed Privacy Standards, we have taken this approach to the extent allowed under the HIPAA statute.

Security

The second principle is Security. Americans need to feel secure that when they give out personal health care information, they are leaving it in good hands. Infor-

mation should not be used or given out unless either the patient authorizes it or there is a clear legal basis for doing so.

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

What do we mean by reasonable steps? The organizations should be required to have in place protective administrative and management techniques, educate their employees about these procedures, and impose disciplinary sanctions against employees who use information improperly or carelessly.

We addressed some of these steps in our Security Standards regulation, implementing the Administrative Simplification mandate under HIPAA.[2] That NPRM laid out a range of approaches for safeguarding the information to which the HIPAA mandate applies. In the privacy NPRM we proposed related steps for safeguarding health information, and we will coordinate these requirements in the final Security and Privacy regulations. However, these regulations will not reach all health information held by health plans and providers. We need legislation to cover all health information that needs this kind of protection.

We don't believe a law can specify the details of these protections because each organization must keep pace with the new threats to our privacy and the technology that can either abate or exacerbate them. But a federal law can require everyone who holds health information to have these types of safeguards in place and specify the appropriate sanctions if the information is improperly disclosed. In our regulations, we have proposed such a "scalable" approach, to reflect the differences in the size and nature of the entities that hold health information. The proposed regulations set forth the basic principles and general criteria for securing health information, and leave the specific steps for meeting these principles to each regulated entity. In this way, each entity can take the steps most appropriate to its size, the nature of the information it holds, and its business practices.

Consumer Control

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

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

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

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

Finally, we recommend a process for patients to seek corrections or amendments to their health information to resolve situations in which innocent coding errors cause patients to be charged for procedures they never received, or to be on record

---

[2] The notice of proposed rule making for Security and Electronic Signature Standards, covering security safeguards for electronic information, was published on August 12, 1998.

as having conditions or medical histories that are inaccurate. The proposed privacy standards follow these Recommendations.

Accountability

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

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

In addition to punishing the perpetrators, we must give redress to the victims. We believe that any individual whose privacy rights have been violated should be permitted to bring a legal action for actual damages and equitable relief. The standard for such actions should not be set so high as to make the right meaningless in practice. Attorney's fees and punitive damages should be available when the violation is particularly egregious. As described more fully below, the HIPAA legislative authority does not allow the regulation to accomplish these goals.

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

Public Responsibility

Just like our free speech rights, privacy rights can never be absolute. We have other critical—yet often competing—interests and goals. We must balance our protections of privacy with our public responsibility to support national priorities—public health and safety, research, quality care, and our fight against health care fraud and abuse and other unlawful activities.

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

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

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

Public Health and Safety

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

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

Research

An important mission for the Department of Health and Human Services is to fund and conduct health research. We understand that research is vitally important

to our health care and to progress in medical care. Legislation should not impede this activity.

Today the Federal Policy for Protection of Human Subjects (the Common Rule) and FDA's Human Subject Protection Regulations protect participants in research studies that are funded or regulated by the federal government. These rules help protect the research subjects while not impeding the conduct of research. To protect patient privacy, we recommend that similar protections should be extended to all research in which individually identifiable health information is disclosed without patient authorization, and not just federally funded or regulated research.

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

Under the Common Rule, if personal identifiers are necessary, an IRB (Institutional Review Board) must review the research proposal and determine whether informed consent is required or may be waived. In order for informed consent to be waived, an IRB must determine that the research involves no more than minimal risk to participants, that the absence of informed consent will not adversely affect the rights and welfare of participants, that conducting the research would be impracticable if consent were required, and that whenever appropriate, the participants will be provided with additional pertinent information after participation. This kind of IRB, privacy board, or a similar mechanism of review should be applicable for all research using individually identifiable health information without a patient authorization, regardless of funding source.

Because the Common Rule was designed for protection of human subjects in general, not specifically with privacy protection in mind, our Recommendations included additional criteria for release of information without the subject's consent. We included those criteria in our proposed rule. We believe that, before an IRB or privacy board can approve disclosure of health information without the subject's consent, it should determine that: the research would be impracticable to conduct without the identifiable health information; the research project is of sufficient importance to outweigh the privacy intrusion that would result from the disclosure; there is an adequate plan to protect the identifiers from improper use and disclosure; and there is an adequate plan to destroy the identifiers at the earliest opportunity, unless there is a health or research justification for retaining identifiers. We have included these additional criteria in the proposed privacy regulation.

PREEMPTION

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

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

This is consistent with the broader approach taken to preemption in the HIPAA statute, both in the insurance reform provisions and the administrative simplification and privacy provisions. For the most part, State laws that go further than the federal law are preserved. We recognize that there are some concerns with this approach. In fact, some of these concerns are recognized in the privacy provisions of the HIPAA statute, which create carve outs from preemptions for state laws governing certain public health functions as well as other specific activities such as fraud and abuse. At the same time, we believe that, if a federal law is sufficiently strong, states will not need to enact additional privacy legislation.

HHS PROPOSED PRIVACY STANDARDS

Process and Status

To assist us in developing the proposed rule, we assembled an interagency team including representatives from all parts of HHS, as well as the Departments of Labor, Defense, Commerce, and Justice, the Social Security Administration, the Department of Veterans Affairs, the Office of Personnel Management, and the Office of Management and Budget. We published the proposed rule on November 3 of

1999; the period for public comment closes, today, February 17, 2000 and we will call upon the same broad team to review and respond to the public comments.

We have also continued the consultations with outside groups that we began in preparing the Recommendations. Since the proposed rule was published, we have meet with over____, and many of these were coalitions representing still more interested parties. We have learned a great deal from these consultations, and will continue fact-finding outreach as necessary based on our review of the public comments.

As of February 15, we had received over 30,000 comments by mail or hand delivered, and roughly 10,000 electronically via the web. Once we have logged in all the comments, we will make them available to the public on our web site. Although we have not set a target date for the final rule, largely because we do not know how many comments we will receive, we intend to continue to make this regulation a top priority and publish a final rule as soon as possible, consistent with our responsibility to take the public comments into account.

The proposed rule is based on the five key principles outlined above, from the Secretary's recommendations: Boundaries, Security, Consumer Control, Accountability, and Public Responsibility. To the extent possible under the HIPAA statutory authority, it implements these principles as discussed in detail in the Recommendations.

Because the proposed rule is widely available, we will not repeat it here. Rather, we will highlight a few areas in which we are unable to implement our Recommendation in full due to limitations in the Statutory authority provided under the HIPAA. A summary of the proposed rule is attached, and is available at our web site.

WHY THE REGULATION DOES NOT PROVIDE COMPLETE PROTECTION

Coverage

The Recommendations call for legislation that applies to health care providers and payers who obtain identifiable health information from individuals and, significantly, to those who receive such information from providers and payers. The Recommendations follow health information from initial creation by a health plan or health care provider, through various uses and disclosures, and would establish protections at each step: "We recommend that everyone in this chain of information handling be covered by the same rules."

However, the HIPAA limits the application of our proposed rule to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act (the "covered entities"). Unfortunately, this leaves many entities that receive, use and disclose protected health information outside of the system of protection that we propose to create.

In particular, the statute does not directly cover many of the persons who obtain identifiable health information from the covered entities. In the rule we are, therefore, faced with creating new regulatory permissions for covered entities to disclose health information, but cannot directly put in place appropriate restrictions on how many of the likely recipients of such information may use and re-disclose such information. For example, the Secretary's Recommendations proposed that protected health information obtained by researchers not be further disclosed except for emergency circumstances, for a research project that meets certain conditions, and for oversight of research. In the rule, however, we cannot impose such restrictions directly on researchers; instead, we propose that plans and providers obtain proof of IRB or privacy board approval of the research protocol. Additional examples of persons who receive health information but whom we cannot reach with the regulation include employers, workers compensation and life insurance issuers, and law enforcement officers. We also do not have the authority to directly regulate many of the persons that covered entities hire to perform administrative, legal, accounting, and similar services on their behalf, and who would obtain health information in order to perform their duties. This inability to directly address the information practices of these groups leaves an important gap in the protections provided by the proposed rule.

In addition, only those providers who engage in the electronic administrative simplification transactions can be covered by this rule. Any provider who maintains a solely paper information system would not be subject to these privacy standards, thus leaving another gap in the system of protection we propose to create.

The need to match a regulation limited to a narrow range of covered entities with the reality of information sharing among a wide range of entities led us to consider severe limits on the type or scope of the disclosures that would be permitted under the proposed regulation. The disclosures we propose to allow, however, are nec-

essary for smooth operation of the health care system and for promoting key public goals such as research, public health, and law enforcement. We decided that, on balance, such severe limits on disclosures could do more harm than good. The only appropriate way to fill this gap in protection is with legislation that regulates not just the disclosing plans and providers, but also those receiving health information from plans and providers.

Enforcement

Requirements to protect individually identifiable health information must be supported by real and significant penalties for violations. We recommend federal legislation that would include punishment for those who misuse personal health information and redress for people who are harmed by its misuse. We believe there should be criminal penalties (including fines and imprisonment) for obtaining health information under false pretenses, and for knowingly disclosing or using protected health information in violation of the federal privacy law. We also believe that there should be civil monetary penalties for other violations of the law, and that any individual whose rights under the law have been violated should be permitted to bring an action for actual damages and equitable relief. Only if we put the force of law behind our rhetoric can we expect people to have confidence that their health information is protected, and ensure that those holding health information will take their responsibilities seriously.

In HIPAA, Congress did not provide sufficient enforcement authority. There is no private right of action for individuals to enforce their rights. In addition, we are concerned that the penalty structure does not reflect the importance of these privacy protections and the need to maintain public trust in the system.

For these and other reasons, we continue to call for federal legislation to ensure that privacy protection for health information will be strong and comprehensive.

CONCLUSION

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

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

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

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

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

Proposed Standards for Privacy of Individually Identifiable Health Information

Statutory Requirement

Section 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, enacted August 21, 1996, requires that, if legislation establishing privacy standards is not enacted "by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act."

The statutory deadline for Congress to enact legislation was August 21, 1999. Absent legislation, HHS has developed its proposed rule.

Overview

The proposed rule would:

•

• allow health information to be used and shared easily for the treatment and for payment of health care;

• allow health information to be disclosed without an individual's authorization for certain national priority purposes (such as research, public health and oversight), but only under defined circumstances;

• require written authorization for use and disclosure of health information for other purposes, and
• create a set of fair information practices to inform people of how their information is used and disclosed, ensure that they have access to information about them, and require health plans and providers to maintain administrative and physical safeguards to protect the confidentiality of health information and protect against unauthorized access.

Scope

a. Entities covered by the proposed rule

• Health care providers who transmit health information electronically
• Health plans
• Health care clearinghouses

b. Health information covered by the proposed rule ("Protected health information")

• Protection would start when information becomes electronic, and would stay with the information as long as the information is in the hands of a covered entity.
• Information becomes electronic either by being sent electronically as one of the specified Administrative Simplification transactions or by being maintained in a computer system.
• The paper progeny of electronic information is covered; the information would not lose its protections simply because it is printed out of the computer.
• HIPAA protects the information itself, not the record in which the information appears.
• The information must be "identifiable." If the information has any components that could be used to identify the subject, it would be covered.

General rules

We propose that covered entities be prohibited from using or disclosing health information except: as authorized by the patient, or as explicitly permitted by the regulation. The regulation would permit use and disclosure of health information without authorization for purposes of health care treatment, payment and operations, and for specified national policy activities under conditions tailored for each type of such permitted use or disclosure.
• The amount of information to be used or disclosed would be restricted to the minimum amount necessary to accomplish the relevant purpose, taking into consideration practical and technological limitations.
• There would be exceptions for situations in which assessment of what is minimally necessary is appropriately made by someone other than the covered entity (e.g., such as when an individual authorizes a use or disclosure of information, or when the disclosure is mandatory under another law).
• We would allow covered entities to rely on requests by certain public agencies in determining the minimum necessary information for certain disclosures.
• Under the principle of minimum necessary use, if an entity consists of several different components, the entity would be required to create barriers between components so that information is not used or shared inappropriately.
• To encourage covered entities to strip identifiers from health information when it is possible to do so, we would permit a covered entity to use and disclose such de-identified information in any way, provided that:
• it does not disclose the key or other mechanism that would enable the information to be re-identified, and
• it has no reason to believe that such use or disclosure will result in the use or disclosure of protected health information (e.g., because the recipient has the means to re-identify the information).
• We would treat the key to coded identifiers the same as the information to which it pertains. A covered entity could use or disclose a key only as it could use or disclose the underlying information.
• We would permit covered entities to disclose protected health information to persons they hire to perform functions on their behalf, where such information is needed for that function. These "business partners" would include contractors such as lawyers, auditors, consultants, health care clearinghouses, and billing firms, but not members of the covered entity's workforce.
• Except where the business partner is providing a treatment consultation or referral, we would require covered entities to enter into contracts with their business partners and would require the contracts to include terms to ensure that the protected health information disclosed to a business partner remains confidential. Busi-

ness partners would not be permitted to use or disclose protected health information in ways that would not be permitted of the covered entity itself. We use the contract as a tool for protecting information, because the HIPAA does not provide legislative authority for the rule to reach many such business partners directly.

- The uses and disclosures permitted by this rule would be exactly that—permitted, not required. For disclosures not compelled by other law, providers and payers would be free to disclose or not, according to their own policies and principles. At the same time, nothing in this rule would provide authority for a covered entity to refuse to make a disclosure mandated by other law.
- Only two disclosures would be required by this proposed rule: disclosure to the subject individual pursuant to the individual's request to inspect and copy health information about him or her, and certain disclosures for the purposes of enforcing the rule.
- Health information covered by the proposed rule generally would remain protected for two years after the death of the subject of the information, subject to certain exceptions.

Disclosures without authorization for health care treatment, payment, and operations

- Covered entities could use and disclose protected health information without authorization for treatment, payment and health care operations. This would include purposes such as quality assurance, utilization review, credentialing, and other activities that are part of ensuring appropriate treatment and payment.
- Individuals generally could ask a covered entity to restrict further use and disclosure of protected health information for treatment, payment, or health care operations, with the exception of uses or disclosures required by law. The covered entity would not be required to agree to such a request, but if the covered entity and the individual agree to a restriction, the covered entity would be bound by the agreement.

Uses and disclosures with individual authorization

- Covered entities could use or disclose protected health information with the individual's authorization for almost any lawful purpose.
- We would prohibit covered entities from conditioning treatment or payment on the individual agreeing to disclose information for other purposes, and require the authorization form to state this prohibition.
- While the provisions of this proposed rule are intended to make authorizations for treatment and payment purposes unnecessary, some States may continue to require them. Generally, this rule would not supersede such State requirements. However:
- the rule would impose a new requirement that such State-mandated authorizations must be physically separate from an authorization for other purposes described in this rule.
- the authorization would have to meet the rule's requirements for the content of such authorizations (although a state law could require that an authorization contain additional provisions).
- We would require authorizations to specify the information to be disclosed, who would get the information, and when the authorization would expire. If an authorization is sought so that a covered entity may sell or barter the information, the covered entity would have to disclose this fact on the authorization form.
- Use or disclosure of information by the covered entity inconsistent with the authorization would be unlawful.
- Individuals could revoke an authorization.

Permissible uses and disclosures for purposes other than treatment, payment and operations

- Covered entities could use and disclose protected health information without individual authorization for the following national priority activities:
- Oversight of the health care system, including quality assurance activities;
- Public health, and in emergencies affecting life or safety;
- Research;
- Judicial and administrative proceedings;
- Law enforcement;
- To provide information to next-of-kin;
- For identification of the body of a deceased person, or the cause of death;
- For government health data systems;
- For facilities' (hospitals, etc.) directories;
- To financial institutions, for processing payments for health care; and

- In other situations where the use or disclosure is mandated by other law, consistent with the requirements of the other law.
- Specific conditions would have to be met in order for the use or disclosure of protected health information to be permitted. These conditions are tailored to the need for each specific category listed above and to the types of organizations involved in such activities.

Individual rights

The proposed rule would provide several basic rights for individuals with respect to protected health information about them. Individuals would have:

- The right to receive a written notice of information practices from health plans and providers. The notice must describe the types of uses and disclosures that the plan or provider would make with health information (not just those uses and disclosures that could lawfully be made). When plans and providers change their information practices, they would also have to update the notice. Plans and providers would be required to follow the information practices specified in their most current notice.
- The right to obtain access to protected health information about them, including a right to inspect and obtain a copy of the information.
- The right to request amendment or correction of protected health information that is inaccurate or incomplete.
- The right to receive an accounting of the instances where protected health information about them has been disclosed by a covered entity for purposes other than treatment, payment, or health care operations (subject to certain time-limited exceptions for disclosures to law enforcement and oversight agencies)

Administrative requirements and policy development and documentation

This proposed rule would require providers and payers to develop and implement basic administrative procedures to protect health information and the rights of individuals with respect to that information.

- Covered entities would be required to maintain documentation of their policies and procedures for complying with the requirements of the proposed rule. The documentation must include a statement of the entity's practices regarding who would have access to protected health information, how that information would be used within the entity, and when that information would or would not be disclosed to other entities.
- Covered entities would be required to have in place administrative systems, appropriate to the nature and scope of their business, that enable them to protect health information in accordance with this rule. Specifically, covered entities would be required to:
- designate a privacy official;
- provide privacy training to members of its workforce;
- implement safeguards to protect health information from intentional or accidental misuse;
- provide a means for individuals to lodge complaints about the entity's information practices, and maintain a record of any complaints; and
- develop a system of sanctions for members of the workforce and business partners who violate the entity's policies.

Scalability

We propose privacy standards that covered entities must meet, but leave the detailed policies and procedures for meeting these standards to the discretion of each covered entity.

- We intend that implementation of these standards be flexible and scalable, to account for nature of each covered entity's business, and the covered entity's size and resources. We would require that each covered entity assess its own needs and implement privacy policies appropriate to its information practices and business requirements.
- The preamble to the proposed rule will include examples of how implementation of these standards are scalable.

Preemption

Pursuant to HIPAA, this rule will preempt state laws that are in conflict with the regulatory requirements and that provide less stringent privacy protections, with specified exceptions for certain public health functions and related activities.

Enforcement

- Under HIPAA, the Secretary is granted the authority to impose civil monetary penalties against those covered entities which fail to comply with the requirements of this regulation.
- HIPAA also established criminal penalties for certain wrongful disclosures of protected health information. These penalties are graduated, increasing if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain.
- Civil monetary penalties are capped at $25,000 for each calendar year for each standard that is violated.

What this proposed rule does not do

- The HIPAA limits the application of our proposed rule to the covered entities. It does not provide the authority for the rule to reach many entities that receive health information from these covered entities, so the rule cannot put in place appropriate restrictions on how such recipients of protected health information may use and re-disclose such information.
- Any provider who maintains a solely paper information system cannot be subject to these privacy standards.
- There is no statutory authority for a private right of action for individuals to enforce their privacy rights.

Chairman THOMAS. Thank you, Dr. Hamburg.

In my opening comments I indicated some concern about the timeline for issuing final regulations and it has become something of, if not a joke, at least a model for us to be concerned about. I am referring to the 1993 legislation that is commonly referred to as Stark II in terms of self-referral, compensation and ownership. I have long thought that the ownership portion made complete sense and that portion has not been too difficult to get a handle on. But you have been chasing the elusive butterfly of compensation for seven years now and you still have not issued final regulations.

I am guessing, as you indicated with all of the concerns and frustrations with the underlying legislation, although I think setting up some parameters that you bumped into, some of which you seemed to be able to knock over and keep going for whatever reasons and decided to stop with the others that were in the legislation, it might be ultimately a useful thing so that we can at least focus on friction areas or problem areas. But in the Stark II legislation, seven years no final regulation in the area of compensation.

I personally believe that if you do issue final regs all they will be will be intermediate final regs which will then have to be fine-tuned by legislation and in fact I am trying to short-circuit that.

That is by way of a preamble of saying, I do not think we can let that history be a model in this particular area. There have been attempts, primarily on the Senate side, to move forward legislatively. I want to underscore the gratitude from myself, and based upon the comments, shared by other members of this subcommittee on your willingness to jump in and move relatively expeditiously.

However, you have come up with just a couple of points that I would like to highlight in terms of the difficulty and invite your response. I do not want to go into an extensive question and answer period. I will submit in writing to you so you can feel comfortable in commenting on them about two dozen additional questions, some

of which I might have ordinarily asked, so that we can better understanding your thinking in particular areas.

So the questions that I would ask you are kind of general but highlight the concerns in particular areas. You indicate that you have made a cost estimate of this particular legislation of about $3.8 billion. Often times we joke about how close something is for Government work. So if you are off by a factor of two, that is close enough for Government work. A factor of three to five, that is probably sloppy Government.

But what we are going to hear is testimony that you may be off as much as seven, eight, 10 times the amount of money, in part because, I believe, of the ripple effect to secondary structures otherwise known, for example, as business partners who are covered entities and that you require a level of knowledge and performance on a ripple out aspect that I have a hard time believing was part of your estimate contained in the $3.8 billion.

Do you have a comfort level that the $3.8 billion is a pretty complete cost analysis on what will be hopefully, with minor adjustments, the final rule? Or are you planning on doing, based upon the comments submitted, a more complete cost analysis before publishing a final rule?

Dr. HAMBURG. That, of course, is a very important question. We had put forward a cost estimate that spanned a range, about $1.6 to $6.3 billion, but recognized that there were areas of activity contained within the proposed regs where we did not have very good data for doing cost analysis, and one of the things we asked for in the process of comment was for additional data that could help enlighten these concerns.

There have been cost estimates that have been put out and other evaluations that we think are quite inflated, that cost out activities that in fact are not contained within our regs. Of course, we recognize that we put forward a proposed reg on a complex issue for which there are many, as you say, ripple effects, many interested parties, and the final regulation will be shaped very much by the kinds of comments that are coming in.

We will be looking very closely the cost issues but we do believe that the cost estimates that have been put forward by some other entities really do not crosswalk with what is in the reg as it currently exists. We will look closely at those so that we can compare how they got to their numbers, how we got to our numbers, and we have been engaged in that. We do need to look at some areas where we did not feel we had adequate data and see if new data sheds new light.

Chairman THOMAS. I do not want anyone to assume that what is driving this is a cost consideration. It is just that I would like to have it as accurate as we can because, frankly, when you move to these other business partners as covered entities—I mean, there are existing relationships—you are going on top of, in many instances, State laws. And of course, there are preexisting State licensing requirements that deal with professional conduct.

It just seems to me that as you extend this umbrella of a partial Federal structure as you do, it is going to require necessarily renegotiations of a number of contracts which may in fact either impede care that is out there or produce some disruption in the struc-

ture which will have dollar value to it. It may be extremely difficult to put a value on that.

But one of the questions that I would have and you may want to respond briefly now but it will be a part of the written question area is, did you consider and why did you reject dealing with business partners being required to certify that they comply with the regulations, not take one of the covered entities and hold them liable for a business partner's failure to comply? Some degree of certification would partially shift the responsibility.

Now I know you are limited by the legislative window that is available to you. Would this be an area in which clearly from a legislative point of view we would want to focus in some detail?

Dr. HAMBURG. I think we all share the concern that these privacy protections be meaningful, real, and enduring, and our desire in addressing the business partners question was to ensure that, if we had privacy protections on the covered entities, that information that they would be sharing with business partners would continue to receive the same protections that the consumers would now have the expectation of having.

Because of, as you say, the constraints of the statute, we cannot directly regulate those business partners, but we felt that we were trying to achieve in the proposed reg just what you were asking about: the certification that they would comply with the same privacy protections, and through the contractual mechanism we thought that could be achieved.

Chairman THOMAS. One of the real concerns I have shared by the way by a colleague on this committee, Ben Cardin, as we have attempted to move forward in concert in a bipartisan way in dealing with this area is that although there is some great desire to maintain a State structure and a Federal structure and your goal was to build a floor while allowing individual States to have ceilings.

But the very fact that you have got to reconcile this kind of crazy quilt of relationships, especially when you throw in a number of phrases that deal with minimums, in what way do they relate to State structures, that perhaps it just might be a better way of looking at this whole area if you do not say that given today's world, paper or electronic, that a Federal preemption providing a uniform structure across all States, one, might not be a better way to afford protection and confidentiality. But two, would eliminate this extremely difficult job of trying to mesh from a floor to a ceiling, different State as well as now, new Federal regulations and impositions.

Do you personally believe that the approach that the legislation requires you—that is, you could not offer Federal preemption—that structure is in fact the better way to go?

Dr. HAMBURG. This has been the topic of great debate and many well-informed thoughtful thinkers weighing in on differing sides. I think what we are trying to achieve is, as you say, the establishment of a clear set of protections in which the consumers can have confidence. If that were to be achieved I think States would feel less of a need to fill in the gaps and create their own privacy laws.

There are, however, different concerns in different States. There are different issues that emerge. There are new technologies that

impact different places differently. So to allow States to continue to have some flexibility as they see fit to tailor the law to suit their needs seems like a reasonable approach. But I do think that having comprehensive national privacy legislation would go very far in reducing this patchwork approach.

Chairman THOMAS. So you have firmly established yourself on the one hand, and then on the other. One of the frustrations of this job is that I almost always want to inquire if any agency that is going to testify has a one-armed member of the agency so that when they come they would not be able to be on the one hand and on the other.

For example, you actually propose to preempt State law, do you not, in this regulation?

Dr. HAMBURG. We propose that where the regs would be more stringent that it would—

Chairman THOMAS. Preempt State law.

Dr. HAMBURG. —override State law.

Chairman THOMAS. Preempt State law.

Dr. HAMBURG. Yes.

Chairman THOMAS. Override State law. Say that a State in its wisdom in making a decision in this was not very wise and we are going to impose our regulation in this area. So you already have what I consider to be taken the first step. You believe there are States whose laws should be preempted by this Federal standard. But then you say you are going to allow States to continue to make regulations in particular areas.

We are going to enter an area, in large part based upon the publicity of data that is somewhat aged at the current time, in the area of medical errors with the publication of the Institute of Medicine's, To Err is Human. Would not your proposal, that is preempt some areas and not preempt others, invite States to then go ahead and pass laws in terms of restricting the ability to collect information which we might consider to be essential in removing what everyone says they want to remove, and that is the up to 100,000 deaths a year through medical errors?

I would like you, if you could succinctly as possible, explain the Administration's position that in certain areas we want uniformity, but in the most sensitive, most extreme areas where we have got to gather the data that is most important, you think it is best to have a crazy quilt of State laws controlling the flow of this information. What is the rationale behind that approach?

Dr. HAMBURG. I think that, as I have articulated already, the approach that is being put forward is to create a strong foundation of privacy protection that would capture what is believed to represent a firm foundation, and then allow States the flexibility to respond to the issues that arise within their States and from their specific constituencies, and respond to—

Chairman THOMAS. Including a strong feeling that certain information, notwithstanding the fact we believe it is necessary by building that floor, should not be allowed to flow and therefore we are going to restrict it?

Dr. HAMBURG. I think that States should not be prevented to respond to needs that they believe have not been addressed, to respond to emerging concerns, and to respond—

Chairman THOMAS. You started off your statement by indicating that just like freedom of speech it is not absolute, and that in fact in some areas individual rights need to be weighed in relationship to the public's right to know and I guess public health is one of the better areas. My concern is that you begin to get into this thicket very clearly with the Administration's approach in which we are going to have to play catch-up, and as soon as these regulations become final, if they do, there is no question in my mind that a number of State legislatures will begin to move.

They are not moving as rapidly now—Minnesota being one of the prime examples in terms of the enormous difficulty that an institution with as much as prestige as the Mayo Clinic has, has done its darnedest to get the private agreement of individuals, which is the requirement of the Minnesota law. And the foundation for the excellence of medicine at the Mayo Clinic is the epidemiological studies in which they are now looking at a 3 percent hole in their information. Somebody might say, gee, 97 percent is pretty good. As most of know in terms of collecting data or doing research, it is not. It is a hole in the data that makes the data sometimes absolutely useless.

Very concerned about the attempt to create a structure which in fact will expedite our inability to go where we need to go, especially in the area, for example, of medical errors.

Let me give you just one example in terms of the rule that I have some concern about, because the proposed rule prohibits the disclosure of research information unrelated to treatment without an individual's authorization. Would you at least, since obviously you have a medical background and I do not, indicate to me that there are sometimes disagreements as to what information is or is not related to treatment? That a phrase, unrelated to treatment, is at least open to differing interpretation?

Dr. HAMBURG. To respond to the broad comment that you made about access to information for research, there are within the proposed regs clear issues raised about that, and an indication that there should be circumstances in which researchers can receive data about individual patients, but that there needs to be a process that is clearly defined and a set of standards that are met in terms of that information being made available and then how it is handled. Not all research requires patient identifiers with that information. So when you do not need to use patient identifiers, that clearly provides more patient protection.

With respect to your question of is there a fuzziness around whether the information that would go to a researcher is relevant to treatment—

Chairman THOMAS. No, not relevant. Unrelated. Not relevant. Unrelated is the term that is used in the proposed reg.

Dr. HAMBURG. I am not completely sure that I understand your question. If you are asking whether it will have—

Chairman THOMAS. I will submit it in writing and you can have others who were more directly involved in writing it—

This is the kind of dilemma that I would like to leave with you and then I will allow my colleague some questions. What would the department do—just as a for instance, what would the department do if a State passed a privacy law that enabled providers to with-

hold what you considered to be critical public health information? Now again, sometimes this information is in the eye of the beholder.

Or for example, that enabled providers to frustrate a Federal anti-fraud investigation. Not related to public health but related to an anti-fraud investigation. Is it still the Administration's position that in these particular instances the sovereign would be able to go in and overturn the State law and overturn the State law and get the information they thought was important?

Dr. HAMBURG. I think the proposed rule makes clear that where there are existing laws that require certain information be made available, such as with respect to public health, that information would be made available.

Chairman THOMAS. No, the State passed a law saying it was not going to be provided. So you would go in and say, notwithstanding what you may assume to be a State right, we are going to say no in this area; is that what you said?

Dr. HAMBURG. For critical issues such as—

Chairman THOMAS. Who defines the critical issue?

Dr. HAMBURG.—public health would be—

Chairman THOMAS. Who defines the critical issue? Does not the sovereign, does not the Federal Government define it, as you have done in this regulation in preempting certain State laws that you thought did not reach a particular level associated with what you considered to be appropriate?

Dr. HAMBURG. We are, as I said, going to be reviewing all the comments that come in. The final reg is not established yet, but it is the clear intent as we move forward toward shaping that final regulation to ensure that such critical national security, national health protection needs are not inhibited—

Chairman THOMAS. And that is a good position to rally around, because national security health needs—but I also mentioned anti-fraud. Would you then push your ability to overturn State laws if in withholding information it inhibited the inspector general or others? Because this majority has passed more than 65 specific assistances in going after fraud and abuse which the Administration has rightly touted has produced more than $10 billion of savings over the last several years in using the tools that we have provided you in stopping fraud and abuse.

But if a State passed, based upon the desire to withhold personal information, which may in fact conflict with your ability to get at anti-fraud, then would you not also want to move in that area in terms of preemption?

Dr. HAMBURG. I think it has been very clear that on the public responsibility side of this, public health as well as the fraud and abuse areas, certain law enforcement needs, et cetera, have to balanced against the other protections and we feel that is a critical component of what we are trying to achieve.

Chairman THOMAS. All I am saying is that clearly I could name any number of specific instances in which you would choose for the sovereign; that is, preempting the State. My argument is, that is a really slippery slope. Set up a structure and then have this conflict over a number of years over something as sensitive as patient

medical records, and how they are handled. And the crazy quilt that your basic structure would produce across the country.

Perhaps we ought to just face the issue—now this is a Republican talking about Federal preemption. We should just face the issue that it ought to be done in a way that gives us the maximum opportunity to afford uniform security protection, confidentiality. And that it ought to be a Federal preemption rather than your Federal floor over where today you think it is important to preempt State laws, but where tomorrow there is no question you will find you are put in a choice situation in which you choose to preempt State laws willy-nilly, which means you drive other States to pass laws based upon the reaction to the Federal move.

I just think that direction is fraught with danger in providing a uniform appropriate data collection for research, for error correction, commensurate with protecting the individual's right to confidentiality on their medical records.

The gentleman from Washington.

Mr. MCDERMOTT. Thank you, Mr. Chairman. I want to address my questions both to you, Dr. Hamburg, and also Mr. Claxton, because I think you had something to do with the writing. You are not sitting there for no reason. So whichever of you feel is you are the best to answer the question I think it would be helpful.

In response to—it is interesting to listen to the chairman. I do not often hear you suggesting Federal preemption, big Government. So it is always interesting to hear.

Chairman THOMAS. Uniform Government.

Mr. MCDERMOTT. Yes. I am sorry. It may become big, right?

Chairman THOMAS. Uniform big is better than non-uniform big.

Mr. MCDERMOTT. When the bill was written—

Chairman THOMAS. In the protection of individual rights.

[Laughter.]

Mr. MCDERMOTT. I did not interrupt you at all. I let you have your go here.

The issue of the bill having been written giving you a Federal preemption, you wrote your regulation with that in mind. The Congress said you are to preempt State laws; is that correct?

Dr. HAMBURG. With respect to the—yes.

Mr. MCDERMOTT. To the narrow areas that are covered by this regulation.

I make that point because on the one hand we said, preempt State laws and then we tied your hands. We said, you cannot look at the whole area of privacy, you just have to look at this one little narrow area. Coming from having a background in a State legislature, I do not know how many times we had to adjust our laws to fit a Federal law. It was a constant part of being a State legislator was always making adjustments.

So I think the chairman raises an issue, but the reason we are here on this issue at the national level is because it is not being done at the local level in a uniform way. I think there are only 28 States that allow patients to actually look at their own record. You have a legal right to look at your record. In many States you cannot go in and say, I want to see what is in my record.

So it seems to me that is a big part of what you are trying to do here is to set a floor. Now the question is, how high you set the

floor as to how much you are going to get in the State legislature. Is that your anticipation?

Dr. HAMBURG. I think that you have framed it exactly right.

Mr. MCDERMOTT. Because I listen to this and I think to myself, there is a specific issue that, this business about why you went at the business partners the way you did. The law says that you can regulate health plans, providers, certain providers, and clearinghouses. And anybody who knows anything about the health care delivery system realizes there is a whole other series of entities out there that can use, have used for a variety of reasons, either for research or for marketing purposes, this data.

Your job was—then they tied our hands with only three, how do we get at these things? That is the reason why you have the business partner section in there; is that correct?

Dr. HAMBURG. Absolutely. I think it also underscores one of the reasons why we fundamentally believe that while we have made a very good faith effort in trying to achieve privacy protections through this reg, that comprehensive national legislation will enable a much broader and more protective approach.

Mr. MCDERMOTT. If you had not reached out through this indirect mechanism of saying that a health care provider or whatever, or a clearinghouse has to have a contract with their business partners about this issue, it essentially would be a loophole big enough to drive—I do not know, anything could fly through it, if I understand—

Dr. HAMBURG. I think that is right, and we would not want to undermine the public confidence in the protections we are trying to put forward for them by allowing surrogates of the covered entities to do exactly the kinds of things with their health information that we are trying to prohibit through the proposed reg.

Now we certainly have heard a lot of concerns about how this concept of reaching to the business partners should be structured and we will be going over the comments very carefully and trying to think that through, because we recognize from important partners that this is an arena that raises concerns about additional burden, additional cost, additional liability, and we have to look at that carefully and take those concerns into consideration.

But we do feel that we cannot simply put forward protections that would address the covered entities and not recognize that, as you say, the information goes out in many different directions. That we have a very complex health care system and many people are involved, and that our reg only formally has the power of enforcement and authority over a very circumscribed element.

Mr. MCDERMOTT. Can I ask you a question that I was sitting here thinking about? If you have an HMO and you have all this data about your patients, this regulation would prohibit you from selling that in some kind of commercial means to health marketing or to wellness whatever or any other entity outside, would it not?

Dr. HAMBURG. Without specific patient authorization.

Mr. MCDERMOTT. Now if you have a wholly owned subsidiary and you transfer it to them, can they then put it out?

Dr. HAMBURG. If it would be to be used for marketing and related activities it would still, even if it was another entity that was

part of this umbrella covered entity, it would still require specific patient authorization for those purposes.

Mr. MCDERMOTT. But if you spun off—because of the business partners question or is it because it is part of one entity?

Dr. HAMBURG. Any use for marketing would require the patient authorization.

Mr. CLAXTON. In your case, because it is part of one entity.

Mr. MCDERMOTT. I am sorry?

Mr. CLAXTON. In your example it is because it is part of one entity.

Mr. MCDERMOTT. Part of one entity.

Mr. CLAXTON. If they spun it off—

Mr. MCDERMOTT. Now if they spun it off and it is totally unrelated, has an arms-length relationship with the HMO, it is now our data marketing organization and we have created a new entity, Inc., then they have that information and they can do whatever they wish with it unless you have this contract between the HMO and this arms-length company—

Dr. HAMBURG. Correct.

Mr. MCDERMOTT.—that is marketing the data; is that correct?

Mr. CLAXTON. Assuming that the entity could have gotten it in the first place as a partner. If it is doing something on behalf of the HMO it could have gotten the information in the first place, and then you need the business partner relationship to continue to protect the information.

Mr. MCDERMOTT. So they give this information to a survey company and they are doing work for the HMO, and that would be the relationship. Then whatever they did with it after that is their own business unless you have this contract.

Dr. HAMBURG. Correct.

Mr. MCDERMOTT. That is why I think it is important that the way we wrote the law you had no other way to get at that relationship, if I understand correctly what you were trying to do.

Dr. HAMBURG. That is absolutely correct.

Mr. MCDERMOTT. Now when you look at the whole question of assuring—

Chairman THOMAS. The gentleman's time has expired. We will move to the other members. If you want to go on for a second round, you can do that.

Mr. MCDERMOTT. Thank you.

Chairman THOMAS. The gentleman from Pennsylvania wish to inquire?

Mr. ENGLISH. I do, Mr. Chairman, and I appreciate the opportunity. Secretary Hamburg, reviewing these regulations which I think address one of the more challenging issues we in Congress have to face this year I wonder, we can all agree on the need to prohibit disclosure of patient information as a central tenet of protecting confidentiality. It is obviously disclosure of information that patients are rightly concerned about.

However, this rule, this proposed rule attempts to limit uses of information without individual authorization, even within a covered entity such as a hospital. Question, do you really believe that you know and have included all of the possible current and future appropriate uses of patient information? If this rule had been pro-

mulgated 15 years ago, could you have predicted all of the innovations that the delivery system has today?

Dr. HAMBURG. No. I think, first of all in formulating the reg we tried to think as carefully through all of the many ramifications as well as emerging potential issues. But it is a very complex issue, very multi-layered, and we are hoping through the comment period to broaden our thinking in the short term. In the long term, of course, things are so rapidly changing both in terms of how our health care delivery system is structured, the technology available to support that, and of course the application of new technologies and procedures and the implications raised.

So I think that there is not going to be one set of privacy regs or one comprehensive piece of privacy legislation that will resolve all the issues now and in the future. But what we are trying to do is really put forward a framework for addressing the problems. But we are going to have a dynamic process.

Mr. ENGLISH. I understand, but that is the rub. Would it not be more workable to focus the regulation on disclosure of patient information and not attempt to regulate use, particularly within a covered entity?

Dr. HAMBURG. I think the two are hand in hand. What we are trying to define are the circumstances, how information within a covered entity can be appropriately used and the protections that should apply. Then also there are needs for others outside of that covered entity to access that information and then to clearly define the circumstances under which that will occur and the responsibility on those outside entities or individuals in terms of how they appropriately handle the information.

Mr. ENGLISH. I would like to get your reaction to some general comments that were sent to Secretary Shalala by Pennsylvania's department of health. They put forward the following recommendation. Even though the intent of the regulation is clear concerning what information is allowed to be released absent individual authorization, DOH is concerned that covered entities may react to the regulations by overprotecting information; i.e., not releasing information to a public health entity for one of more of the above purposes.

This would undermine the intent of the regulations as well as core public health functions. DOH will engage in public education efforts and request that HHS take similar steps to make sure the intent of the regulations is conveyed.

Are you prepared to do that kind of a public education effort?

Dr. HAMBURG. I can assure you that the concerns raised by the Pennsylvania Department of Health will be looked at very seriously. On a very personal basis, I was New York City's health commissioner for six years prior to taking this job. Many of the issues they raise are very close to my heart and I have seen it from the other side. So we will be working intensively during this comment review period to look at all of the comments that come in and to address the concerns. But I can assure you that the issues that surround the issues of public health information will get a serious look.

Mr. ENGLISH. I take that as a very important commitment.

One other recommendation they made, they recommend that HHS should indicate, perhaps in the preamble to the regulation, that agencies receiving information for the above—that is public health function purposes—remain bound by existing State laws which govern the use of such information. Do you agree with that and are you prepared to respond?

Dr. HAMBURG. I would like to be able to look at the comment before responding in this forum.

Mr. ENGLISH. Very good. My time has expired, Mr. Chairman, and I will hopefully get another shot. Thank you.

Chairman THOMAS. Thank the gentleman. Although he is not now a member of the subcommittee—his party rules preclude him from doing that—I know his heart is always with us, and it is a pleasure to see the body and mind attached with the heart today. So the gentleman from Maryland, if he wishes to inquire.

Mr. CARDIN. Thank you, Mr. Chairman. I thank you for the courtesy of allowing me to sit in on this panel. This is a very difficult subject. Secretary Hamburg, I applaud your efforts considering the legislative authority that we gave you. It is difficult to do. And considering the amount of public comment that you have received, you are finding out exactly how much interest there is out there and how many people have their own ideas on how they could draft privacy legislation as it relates to medical records.

One thing I think is clear, Mr. Chairman, and that is, we need a bill. It is wonderful that HHS must go forward with a regulation that is required under law. But ultimately, it is going to be important I think for Congress to pass the framework for medical privacy, and to do it in a more comprehensive way then you are allowed to do under the regulation that has been submitted to you. Mr. Chairman, I do want to applaud your efforts to try to bring out a bill on a bipartisan basis because I think the only way we can do this is in a bipartisan way. It is a very sensitive issue to all of our constituents and it cries out for us to get it done right.

I also want to talk just one minute, if I might, about this idea of a Federal floor and people concerned about preemption, or whether we preempt or whatever. I think that is the wrong way to really look at this. We need national standards as to how medical records should be kept so that we protect the identity of individuals. That should be a national standard. There should be no question about that.

The States are clearly going to be involved. There is public health issues. There are public safety issues, and we need to make sure the States have the ability to protect their citizens where it is appropriate. But we also need to have national standards as to when identifiable information can be made available for research, or when it can be made available for payment, or for treatment. I think that is what we are trying to get at, the right balance.

So the question I have for you, Secretary Hamburg, is that one of the issues that we are having a great deal of difficulty is, how do you enforce whatever standards we come up with? How have you done that in your regulations and how do you think is the best way for us to make sure that these standards, whatever standards are developed, that all parties that are affected by it comply with

the standards? And how do you go about making sure that becomes reality?

Dr. HAMBURG. There are a set of enforcement standards that I believe were given to us through the HIPAA statute in terms of our opportunities for enforcement. And that is one of our concerns, one of the reasons why we feel that in fact national legislation would provide benefits that we cannot achieve through the reg process. There are both civil and criminal penalties that can be applied, but in truth, the enforcement teeth we do not feel are fully adequate.

Mr. CARDIN. So will you be coming forward to us with recommendations as to legislative changes as it relates to enforcement?

Dr. HAMBURG. We are hoping to be working closely with you to develop national privacy protection legislation, and within that context addressing the issue of enforcement.

Mr. CARDIN. But you have no specific recommendation at this time?

Mr. CLAXTON. The Secretary's recommendations in 1997 suggested that we thought there should be civil money penalties for violations criminal penalties for knowing and wrongful conduct. And that there should also be private right of action to address the rights of individual whose privacy rights were violated and who suffer damages.

Mr. CARDIN. This should all be Federal, or not?

Mr. CLAXTON. We thought Federal law should have that in place, yes.

Mr. CARDIN. How does that relate to State enforcement?

Mr. CLAXTON. States would have their own penalties if they had laws. We have not commented on the level of State penalties that should exist as far as I know. We have had some discussions with respect to specific issues such as HIV reporting, but nothing broad.

Mr. CARDIN. I take it an awful lot depends on the standards. I know I am asking a difficult question, but I think it is important as we get into this discussion to make sure that whatever system we have come up with is one that there is effective enforcement on so that we can in fact tell our constituents that we are not only telling in law the standards that protect their medical privacy but that it can be enforced.

Thank you, Mr. Chairman.

Chairman THOMAS. Thank the gentleman. I find it ironic that your goal for Federal legislation is to make sure that you have uniform penalties to go after these people, but the standards, the collection of data, the flow of data, the uses of the data above whatever minimum structure you are talking about would not be afforded the same level of concern. The gentleman uses the term standards and I have no quarrel with that as long as they are high enough that in essence they produce a preemption for uniformity.

My goal is to get your folks to look at the need for standardization on the other side of the ledger as to how you deal with this information and not just the side of the ledger that makes sure that when people do make mistakes in confusing crazy quilt structures of not only all the States and the Federal, but that you can wham them with a real good, uniform penalty. I think it has to be

evenhanded on both sides or you do not get the uniform hammer if you do not provide the uniform standard codes and procedures.

Dr. HAMBURG. I can assure you we have heard your message and we understand the rationale that you are putting forward. I think it would be unfair to characterize our position as that we only are interested on the enforcement side for national standards. We very much support your leadership and that of your colleagues in terms of pushing for national legislation that will provide a very firm standard both for how data is utilized, but also how when there are transgressions in terms of appropriate use, we can enforce appropriate behavior.

Chairman THOMAS. My goal is to create a situation in which my friend Ben Cardin and I present to you a proposal that you cannot refuse.

The gentleman from Washington.

Mr. MCDERMOTT. Mr. Chairman, thank you. I want to clarify something because in listening to the chairman's questions at one point it sounded as though States could erect barriers against legitimate national purposes, and my understanding is that your regulation clearly makes Federal preemption in key national priority areas, including oversight and research and public health, that these are areas where the Federal Government is preeminent in those issues. Is that correct, that they can override a lesser State or an obstructive State issue?

Mr. CLAXTON. In the case where there is already a requirement under Federal law to allow access or make reporting there is nothing in the regulation which would resurrect a State barrier to a Federal law.

Mr. MCDERMOTT. So the States could not use regulation in some way that they could get around the Federal regulation?

Mr. CLAXTON. No. For example, there is nothing about our regulation that makes a State law applicable to an ERISA plan, because they already have Federal preemption.

Mr. MCDERMOTT. So you are saying that the purpose of the Congress; that is, looking at fraud and other medical errors and so forth, no State could pass a law that would prevent us from getting the information to do those kinds of researches?

Mr. CLAXTON. As long as the Federal priority was manifested through a requirement on a provider. If a provider has a choice now, the State law could affect that provider's choice. But the provider in that case would not have had to comply with the Federal request anyway.

Mr. MCDERMOTT. Now there is another area where it seems to me that there is a lot of uncertainty, this whole business of the pharmacy benefit managers, and pharmacy programs, and disease management. These are programs that are new. I mean, they have been going for the last four or five, or maybe eight or nine years, and they gather enormous data about what people are taking in this country. Therefore, you could extrapolate what their disease may be. A lot of people are concerned about their ability to have that data and use it in a variety of ways.

Tell me what you did here, and did you consider making it a requirement that before these entities could use this information they had to have a check-off from the patient that they wanted to be

given mailings about X, Y, or Z? If you have diabetes, the pharmacy knows that you have diabetes. Now you then are subject to having that spread all over the place for whatever anybody can think of that they ought to be doing for you. Did you consider putting a restriction or a requirement for a positive, I want to get further information?

Dr. HAMBURG. With respect to the issues you raise, again we are getting lots of comments, different interpretations, people mean different things when they say disease management programs, for example, so that there is going to be a lot of sorting out. But as long as within a covered entity information is being used as part of the ongoing care and treatment of that individual it does not require a specific patient authorization. If it is being used to send out mailings to market new drugs, et cetera, that would be an inappropriate use.

Mr. MCDERMOTT. And that is for medical devices and everything else? Anything anybody would use that for a marketing tool, it is prevented unless there is a specific—

Mr. CLAXTON. What you said is right. I think the difficult issue is trying to address a situation where a provider is rightfully trying to make his or her patient aware of new information or new products that might be beneficial to that patient and where they are actually engaged in marketing where the provider is relatively indifferent but just saying, here is someone who might be interested. Those are hard lines to draw. We are going to look at the comments and do our best.

But the distinction between disease management and marketing is not clear every time, but it is I think something people feel very strongly about being able to distinguish. It might be that the physician has a fairly key role to play in that and we have heard from various sides on this and expect to hear a lot more.

Mr. MCDERMOTT. If the contract that the HHS wants between the covered entities and the contractual ones, the business partners, is that possible to handle that by having a standard contract that you people would draw up and put out there so that each one of the partners or each one of the entities covered would have in hand something to hand to a business partner and say, sign this?

Dr. HAMBURG. I think that there are so many differing types of partners and the requirements in terms of the working business relationship involve different kinds of elements—not all the business partners are doing the exact same things—that it is unlikely that we would develop standard model contract language. We could certainly identify the critical elements of understanding about how data would be handled, and the expectations should be explicit and will be.

We are certainly open to examining the question, but I think model contract language would not be the primary approach because they are not cookie cutter kinds of relationships where one size fits all. But understanding the elements that need to be included should be explicitly defined.

Mr. MCDERMOTT. Thank you, Mr. Chairman.

Chairman THOMAS. The gentleman from Pennsylvania with to further inquire?

Mr. ENGLISH. Yes, thank you, Mr. Chairman. Secretary Hamburg, within your proposed regulation, Section 160.204 outlines the process for requesting exception determinations, and subsection A.1 outlines the process by which a State may request an exception for a particular State law. Our State department of health has characterized this process as particularly burdensome given the multiple confidentiality laws that exist in Pennsylvania.

I am not as familiar with what other States have, but for Pennsylvania this section would require multiple requests for exception. They argue, the department of health argues that request for exception should be required only when a challenge is brought against a particular State law. The presumption should lie with State laws.

What was your philosophy in crafting this provision, and how do you assess the merits of the department of health's argument?

Dr. HAMBURG. I think I will ask Mr. Claxton to address that as he was intimately involved—

Mr. ENGLISH. Mr. Claxton?

Mr. CLAXTON. Thank you. The HIPAA itself sets forth certain areas where State law—where the Secretary has to make a determination whether or not certain State laws are in conflict. We tried to carry out that section as it was in HIPAA. We have gotten a fair number of inquiries about this and tried to clarify it and we are going to look at the comments. To some large extent I think we are constrained by what the statute says, which is that the Secretary can make a determination with respect to State laws in certain areas.

Mr. ENGLISH. I will accept that and I would appreciate any further response you might want to provide in writing.

Mr. CLAXTON. Certainly.

Mr. ENGLISH. Subsection A.4 limits the length of time for an exception to three years explicitly. I would question why it would be necessary, if there has been no change in State law, to require States to reapply for exceptions. Do you have a policy reason for doing that?

Mr. CLAXTON. I do not recall why that is there. We will be happy to respond in writing.

Mr. ENGLISH. If you would be willing, I would appreciate a response in writing on that point as well.

Finally, Dr. Hamburg, in HIPAA the Secretary was instructed to promulgate regulations that are "consistent with the goals of improving the operation of the health care system and reducing administrative costs." Several of the department's provisions significantly increase the amount of administrative procedures for covered entities.

For example, requiring the review of each protected health information request in order to ensure that "minimum necessary standard", requiring significant allocation of resources to contract with and monitor business partners. Do you not think that these requirements would significantly increase the administrative burden for health care organizations, and is there a better way to do this?

Dr. HAMBURG. I think in shaping the proposed reg we have tried very hard to balance what systems need to be put in place to afford appropriate protection with trying to avoid undue burden. As we

have looked at some of the elements that you referred to, our sense is that while it would add in some cases additional administrative activities and some new burden, that in fact in terms of overall costs our estimates suggest it would be less than one-tenth of 1 percent of overall spending for health care when you break it down on a per-patient basis. It really is not an overwhelming additional cost.

You have to think about it in terms of the additional benefits that would accrue in terms of improving quality of care, reducing the likelihood that individuals would not seek appropriate medical evaluation and treatment because of fears of their important, sensitive health information being misused. So it is a very difficult balancing act.

One of the things that we are going to look at very carefully as we review the comments are the inputs that have come in concerning this issue because we want this to be workable. It is a balancing act and it is very complicated, as we all recognize, but it is an area of major focus and concern and it will be reflected in—

Mr. ENGLISH. And I very much appreciate that. Let me say, I am very sensitive to the enormous paperwork burden we are already putting on health care organizations which is distorting some of their decisions and having an indirect and sometimes hidden insidious effect on the quality of health care in this country. So if there is a way of reducing that paperwork burden as you put forward these regulations I think we should be sensitive to that as well.

Thank you, Mr. Chairman, and I appreciate the opportunity to inquire.

Chairman THOMAS. Thank the gentleman. As I stated earlier, any written questions that any members want to submit, we will leave it open till the close of business because there may be additional questions that need to be asked. In listening to the gentleman's questions, a number of individuals would be envious of your ability to inquire on behalf of the State of Pennsylvania because if this goes into effect I am quite sure there are a number of individuals who would love to ask, which is stricter, the Federal or the State, and create some degree of comfort that they are doing the right thing. When I realized that the outer edges of this is ultimately is going to be enforced by trial lawyers, it should give us all pause.

Thank you very much. Good luck in firming it up. I hope we see a product prior to the ongoing, and counting, seven years of attempting to write a final regulation for Stark II. You are going to need all the help you can get. Thank you very much, Dr. Hamburg, Mr. Claxton.

Dr. HAMBURG. Thank you.

Chairman THOMAS. The next panel, which I guess on an issue like this could extend for row after row after row of witnesses who believe they are going to be impacted by this regulation, and obviously our inability to accommodate it, I do believe that we have got a pretty good cross-section with this panel. We have Dr. William Plested who is a member of the board of trustees of the American Medical Association, obviously an interested party; Ms. Alissa Fox, executive director for legislative policy, Blue Cross-Blue Shield; Janlori Goldman, director of the health privacy project, Institute

for Health Care Research and Policy at Georgetown University; Mary Grealy, president, Healthcare Leadership Council, a consortium of a number of interested partes; and then Dr. Stephen Ober, who is president and chief executive officer of Synergy from Waltham, Massachusetts who is an active player in the transmission of data and who had quite interesting testimony.

Dr. Plested, we will just start with you and then move across the panel. Your written testimony will be made a part of the record and you can address us in the time that you have, which will be five minutes, to give us any flavor of your concern, interest, passion, et cetera.

STATEMENT OF WILLIAM G. PLESTED, III, M.D., MEMBER, BOARD OF TRUSTEES, AMERICAN MEDICAL ASSOCIATION

Dr. PLESTED. Mr. Chairman and members of the committee, my name is Dr. Bill Plested. I am a practicing vascular surgeon from Santa Monica, California, and a member of the AMA Board of Trustees. It is an honor to appear before your committee again.

Thank you for inviting the AMA to speak to you today on an issue of overwhelming importance, not only to physicians, but to every person who finds him or herself as a patient. That is, protecting the confidence and trust that patients place in us.

Trust is the foundation of the patient/physician relationship. My patients assume that the private information they discuss with me will be used to benefit them, not to benefit anyone else who may find a way to profit from their personal information.

Frankly, we see signs that patient records are becoming items of commerce. With many groups clamoring for unfettered access to fulfill some alleged compelling need. But perceived need is not a right.

Let me emphasize that, a need is not a right.

Every business, every company, every government body that wants patients private information must be required to make its case to the American people as to why its professed need should override people's most basic right to keep their medical information private. This is AMA policy, and this is the approach that we have adopted in our comment letter to the Secretary of Health and Human Services, in response to her proposed rule on patient privacy.

First, we are concerned about access to patient records without patient's consent, usually without their knowledge. If medical records were stored in our homes, we would have all kinds of protections, the Fourth Amendment or civil and criminal laws, to keep others from getting and using our information without our permission. Today, patients are forced to share private medical information in order to get the very help that they need. In doing so, they are vulnerable to exploitation by unrelated third parties looking simply for profit.

Physicians are unable to stem this tide. We think the Secretary's regulation makes this situation worse and this is unacceptable.

The Secretary identifies a series of "national priorities" where patients' private medical information would be used without their consent. In fact, most of these can be accomplished using de-identified or aggregate information.

If some information must be individually identified, the first question we should ask should be why not get the patient's consent? Are we concerned that a truly informed patient would not give his or her consent? This should certainly give us pause.

On the other hand, if it is not feasible to obtain consent, there should be an objective, accountable way to make this decision for the patient who is unable to do so. If someone wanted access to your medical information, would you not want to know why do they need to know who I am? Do they truly need information linked to my name? What is the alleged benefit and who stands to profit by getting personal information? What risk am I exposed to if such information is disclosed? What kind of security measures are in place to protect my records and make sure that people use them in the way they said they would or that unauthorized people do not have access?

Such a system already exists in Federally funded research programs. The Secretary's proposed rule would expand such an evaluation to all research, regardless of who is funding this, and this is good. But it needs to be expanded. So-called health care operations that do not benefit a specific patient require especially close scrutiny.

Second, we must comment on the irony that all these new administrative burdens and documentation requirements proposed by the Secretary are the result of so-called administrative simplification. The physicians of America are buried in paper with less and less time to spend with our patients. We object in the strongest terms to the bureaucratic school of thought reflected yet again by the Secretary's proposal that requires extensive and repetitive documentation. This kind of redundant paperwork requirement is for the ease of bureaucrats, not for physicians, and certainly not for patients.

This burden would be especially difficult for smaller sized physicians' offices. These paperwork and administrative requirements need to be completely rethought and, if they are implemented at all, they should have a more realistic and flexible information approach for all physicians' offices.

Let me sum up by getting back to our basic point. The patient/physician relationship is all about trust. It must be fiercely protected. Privacy is a precious right. Once it is lost, it can never be retrieved. We must remain focused on the patient as our first concern in any Federal approach to medical records privacy and confidentiality.

Thank you again for the opportunity to present the AMA's viewpoint today.

[The prepared statement follows:]

Statement of William G. Plested, III, M.D., Member, Board of Trustees, American Medical Association

The American Medical Association (AMA), representing approximately 300,000 physicians and medical student members, appreciates the opportunity to submit testimony to the Health Subcommittee of the Ways and Means Committee regarding an issue central to the patient-physician relationship: protecting patient confidentiality. We particularly appreciate the chance to share with you our concerns regarding the Secretary of Health and Human Services' (HHS) proposed rule on patient privacy, for which public comments are due today ("Proposed Standards for Privacy of Individually Identifiable Health Information," 45 CFR Parts 160 through 164, 64 Fed. Reg. 59917 (November 3, 1999)).

Personal health information is used by various entities in the health care delivery system, including hospitals and health plans, for purposes beyond direct treatment planning and claims payment. Each of these entities argues it needs patient-identifiable health information to achieve its legitimate objective; most believe they do not need explicit patient consent to receive and use such information. That philosophy is reflected in the Secretary's proposed rule and preamble. It is a philosophy rejected by the AMA.

The AMA has consistently maintained that an expressed "need" for information does not confer a right. Patient consent continues to be a critical consideration in the use and disclosure of personally identifiable health information. Consistent with AMA's baseline philosophy regarding individual privacy rights, informed consent should be obtained, where possible, before personally identifiable health information is used for any purpose. However, this is clearly not practical or even possible in some instances. In those situations in which patient consent is not feasible, either (a) the information should have identifying information stripped from it or (b) an objective, publicly-accountable entity must conclude that patient consent is not required after weighing the risks and benefits of the proposed use. A local review board system has already been adopted successfully by several parties to the health care system, including physicians, some researchers, a few health plans, and others.

Some parties may reject this principle as too deferential to patients' rights at the expense of administrative feasibility. The AMA believes that this approach properly balances the interests at stake. Furthermore, it is the right thing to do. At a time when the American public is looking to its leaders for a strong stand on patients' rights, any other policy fails patients, their families and their caregivers.

The AMA cannot support the proposed HHS regulation on patient privacy in its current form. The complexity of the task, compounded by the inherent restrictions under the Health Insurance Portability and Accountability Act's (HIPAA) limited grant of regulatory authority, have resulted in a proposed regulation that does not adequately protect patient confidentiality and privacy and that substantially and unacceptably increases administrative burdens for physicians.

The AMA's overarching concerns are as follows:

- that patients' confidential information could be disclosed without their consent for a broad array of purposes unrelated to the patient's individual treatment or payment and extending far beyond the necessary disclosures and uses patients would expect when they seek health care;
- that many holders of patient information who may misuse such information would not be held accountable under the proposed regulation, despite attempts to bring them within regulatory reach by compelling physicians and other covered entities to, in effect, "police" them;
- that physicians will be held liable for the uncontrollable misdeeds of their "business partners," although the physicians themselves are in compliance with the regulation's provisions;
- that the administrative burden and costs of implementing the proposed regulation have not been adequately calculated, and would have a disproportionate impact on small physician offices; and
- that the proposed rule contradicts the intention of its legislative directive under HIPAA to "simplify" health care administration and reduce costs, and does not improve patients' expectation of privacy in the health care system.

Applicability

The proposed regulation does not cover a broad spectrum of entities that are positioned to disclose and misuse confidential patient information. The AMA finds unacceptable the Secretary's attempt to "fill the gap" in its legislative authority by requiring physicians and other health care practitioners to, in effect, "police" others who should be held accountable. Such a proposal is not only inherently unfair, it is also ineffective insofar as patients may be left without any recourse against a party who wrongfully discloses or misuses their confidential medical information.

General rules

The proposed regulation seemingly is more concerned with facilitating the ease of information flow for the broadly defined purposes of treatment, payment, and health care operations than it is with protecting patients' confidentiality and privacy interests. AMA's policy states that "[c]onflicts between a patient's right to privacy and a third party's need to know should be resolved in favor of patient privacy." In the AMA's view, the general rule should begin with preserving confidentiality and privacy and allowing disclosure only when it is ethically and legally justified.

Scalability—The AMA applauds the Secretary's recognition that a "single approach to implementation of these requirements would be neither economically feasible nor effective in safeguarding health information privacy." Though we appreciate the flexibility physicians and other health care practitioners will be accorded in implementing this proposed regulation, we are concerned that a lack of clear guidance inevitably will lead to costly disputes about compliance.

Minimum necessary use and disclosure—We agree with the Secretary's goal of precluding wholesale transfers of complete medical records when only a small portion is pertinent to the patient's current treatment, but believe the proposed rule's solution may be unworkable. In crafting a solution to the question of limiting disclosures, we recommend a requirement for requesters to make the "minimum necessary demand." While physicians could certainly engage the requester in a dialogue regarding what specific information might be needed in any given instance, the liability would be on the requester for seeking prohibited information, rather than on the physician for not adequately divining the motivations of the requester.

Creation of De-Identified Information—The AMA favors any provisions of the rule that would have the effect of creating incentives to "de-identify" medical information. However, we believe the proposed rule would actually create a disincentive to de-identify information. We recommend revising the list of "identifiers" to be removed from the medical record, combined with an explicit prohibition against "linking" or re-identifying without authorization. This will provide entities with a greater incentive to de-identify information, while holding wrongdoers properly accountable.

Business partners—The AMA strongly objects to the proposed rule's approach of holding physicians and other covered entities responsible for certain violations of the rule's requirements by their business partners. As a matter of fairness, the proposal fails. A physician group, for example, could be subject to the full weight of enforcement and sanctions under the regulation for prohibited activity by its business partners, even if the group had no knowledge or control over the practices of its business partner. The AMA objects to these provisions because they present the potential for significant liability for physicians who, themselves, are complying with the regulation's requirements.

Component entities—We believe the proposed regulation should be modified to expressly recognize the necessity of firewalls within businesses or entities that provide health care as a non-core function. Examples might be school health clinics, on-site employee health services offered by businesses or, employers who operate self-funded health plans for their employees. We are particularly concerned about this last category; public polling indicates that people are deeply concerned that their employers are inappropriately accessing their private medical information. Our key concern in these instances is in assuring that firewalls exist between the health provider function and all other elements of the entity.

Uses and disclosures with individual authorization

The AMA strongly supports a requirement for an individual's authorization for most uses of his or her identifiable health information. The Secretary notes, and the AMA agrees, that individuals generally do not recognize that their information may be used for a multitude of purposes beyond their individual care and payment for that care. This fact underlies the AMA's advocacy for a consent requirement for most uses of an individual's private health information.

We strongly object to the provision that would prohibit physicians from seeking their patients' authorization for treatment, payment or health care operations. This provision flies in the face of medical ethics and directly contradicts the Secretary's expressed intent in the preamble, and should be deleted from the rule.

Uses and disclosures for treatment, payment and health care operations without patient authorization

The AMA questions the Secretary's rationale for choosing to construe the terms "treatment" and "payment" so broadly. The definition of "treatment," for example, would include cost containment mechanisms such as case and disease management that go to managing the costs of populations, rather than the health care of an individual.

Patients reasonably expect that the treatment rendered by their physician will be revealed to their health plan or other insurer to pay the claim for benefits. However, patients do not expect, nor do they welcome, unauthorized access to health information disclosed in the context of a confidential relationship for the wide range of purposes HHS believes to be somehow "compatible with and directly related" to treatment or payment.

The AMA strongly opposes any "disease management" language in the proposed rule that is not qualified by requiring the coordination and cooperation of the indi-

vidual's physician. Patients should have the right to consent to-or refuse-participation in disease management programs offered by providers and plans.

The diversity of proposed uses for information advocated by various groups illustrates the inherent difficulty in addressing these evolving functions within any static legislative or regulatory definition. We recommend application of the controlling rule iterated throughout AMA's comment letter: informed consent should be obtained before personally identifiable health information is used for any purpose. For those many functions or circumstances for which patient consent is not feasible, the information would either have to be de-identified to be used, or the decision regarding its use without patient consent would be made by an objective, publicly-accountable process that weighs the risks against the benefits of the proposed use. This should apply to all operational uses of personally identifiable health information that do not go directly to the individual's specific care, as well as research projects that fall outside the purview of an IRB process.

Right to restrict—We believe the "right to request restriction" is an unworkable "consolation prize" for patients who have had their right to consent taken away from them by government fiat. In addition to its ethical flaws, we believe that offering a right to restrict presents the potential to drive a wedge between patients who want to impose further restrictions and providers who cannot agree to such arrangements due to the overwhelming administrative burdens and potential liability that such individual arrangements would entail.

Permissible uses and disclosures for purposes other than treatment, payment and health care operations

The preamble notes that certain "national priority" activities, as well as the "smooth functioning of the health care system," require the extensive use of individually identifiable health information. The AMA believes that the proposed rule weighs far too heavily in favor of those who seek access to patients' private medical information (often the government), with inadequate deference paid to patients' fundamental right of privacy.

Public health—While mindful that we should not create unduly restrictive barriers for public health researchers to access information, the AMA believes that epidemiologic research on public health and problems should be guided by the same principles for, and safeguards on, privacy and confidentiality that apply to all other medical research. These breaches in confidentiality for a public health purpose are no different from any other breach of a patient's confidentiality that benefits others beside the patient, barring imminent public health emergencies.

Health oversight agencies—The AMA agrees with the Secretary that, generally, oversight activities are important to support national priorities; however, we believe that a majority of these activities could be conducted in a manner that is less intrusive and more sensitive to the need to protect confidential patient information. We believe that the definition's sweeping inclusion of virtually all government agencies that may have any connection, albeit remote, to health care may result in widespread fishing expeditions for confidential patient information. Even more troubling, is that the proposed regulation promotes such access knowing that there are few safeguards in place to protect against the government's wrongful disclosure or use.

The AMA strenuously objects to the seemingly unfettered and unauthorized access governmental agencies will be accorded under the proposed regulation as it is currently drafted. We recommend that if identifiable information is used, it should be accompanied by a limitation on further uses or access by other entities. Our chief concern here is that access by health oversight agencies does not become a "backdoor" for law enforcement access.

Judicial and Administrative Proceedings—While the AMA supports the general provisions of this section, we recommend strengthening the language to increase objectivity and to limit subsequent unauthorized use and re-disclosure. An order by a court or administrative law judge provides some opportunity for an objective screening mechanism to balance the interests at stake in the proceeding, and should be required for all access in judicial and administrative proceedings.

Law Enforcement—The AMA believes strongly that the requesting law enforcement entity should be allowed access to medical records only through a court order. Our position is that a strong legal standard, accompanied by a set of parameters on need and use, is essential to protecting not only personal medical information, but the confidence of citizens in their government.

This is not an abstract concern. Physicians and their patients have repeatedly experienced the intrusion of law enforcement into patients' personal medical information when no need for identifiable information is established and no protections are provided. The unfortunate result is less -rather than greater-confidence in the law enforcement and judicial systems of this country.

Governmental Health Data Systems—The AMA strongly objects to the troubling premise seemingly underlying the entire proposed rule, and particularly evident here, that government oversight of the efficiency and effectiveness of the health care "system" is somehow a more compelling national priority than protecting individual citizens' right to privacy. We cannot agree with reasoning wherein the federal government appears to value even marginal increments of administrative efficiency over the basic rights of individuals to protect the privacy of their own health information.

The AMA sees no reason why government's research and policy analysis purposes could not be fulfilled using de-identified individual or aggregate information. Further, if the government believes it requires individually identifiable health information for its particular purpose, it should be required to obtain the individual's consent for such disclosure and use, or to justify the value of the proposed project and the reasons why obtaining consent is impracticable or impossible.

Research—The AMA strongly supports the extension of the Common Rule to all entities conducting human subject research, regardless of their federal nexus, and applauds the Secretary's efforts in this important area. We agree with the Secretary's conclusion that the nexus of federal funding is irrelevant in deciding the question of whether human research subjects should be protected. As a matter of public policy, individuals should be protected if they or their information are the subject of health-related research. The source of the funding should not result in different levels of protection.

Individual rights

The AMA supports the rights of individual to access their medical records, subject to limited exceptions, which is the approach adopted by the Secretary. We believe that the physical record and notes made in treating the patient belong to the physician; however, the information contained in the record is the patient's. Thus, certain rights should attach for both the patient and the physician.

Administrative requirements and policy development and documentation

This provision sets out an extensive series of administrative requirements that physicians and other covered entities would have to incorporate into their practice or business. The AMA has significant concerns about the substantial administrative and financial burdens this might place on physician practices, particularly those smaller practices whose administrative personnel are already stretched to the limit with various governmental and health plan requirements.

The AMA objects in the strongest terms to the school of bureaucratic thought that requires documentation that one is going to do something, followed by documentation that one is doing that same thing, and then requires documentation that the same thing has been done. Physicians and their office staffs are absolutely overwhelmed by current paperwork requirements generated by well-intended, but poorly thought out, regulations. Such redundant documentation requirements are for the administrative ease of compliance officers—not for physicians and certainly not for patients. Masses of documentation allow compliance officers to push their familiar paper and quibble over parenthetical clauses rather than to really investigate to see when a true wrong has been committed.

The AMA recommends that the paperwork and documentation elements of the proposed rule be withdrawn completely and rethought with a more realistic and flexible implementation approach for smaller physician offices. After all, is the goal to actually protect patient privacy, or is it to create paper saying that we do?

Physicians and other licensed health care professionals already use an array of administrative tools to honor existing ethical and legal obligations to keep patient information confidential. We believe that a prudent implementation of the proposed rule's administrative requirements would permit these covered entities to modify these existing tools, rather than requiring them to "reinvent the wheel." The corporate entities that currently do little or nothing to protect patient privacy are those that the proposed regulation should highlight for additional administrative protections. In addition, we believe that the Secretary has not adequately calculated the costs of implementing the administrative requirements under the proposed regulation. We believe the proposed regulation would have a disproportionate impact on small business (individual and groups of physicians and other health care practitioners).

Preemption and Relationship to State Laws

The AMA is deeply concerned that, while the proposed rule suggests that its preemption provision sets a federal "floor" for preemption, a raft of subsequent excep-

tions and qualifiers completely undermine the provision, creating a federal "basement," rather than a federal "floor."

AMA policy supports a preemption provision that preserves more stringent state confidentiality laws, so that federal and state privacy protections would be cumulative. The proposed rule fails to provide due deference to the States.

This section is also flawed by the fact that entities—specifically physicians—regulated by the rule would not be able to independently ask the Secretary for clarification as to which law to abide by. All queries must be presented by the States. Two implementation problems are immediately evident:

(1) physicians who seek to comply with state law, believing in good faith that it is more stringent than the federal standard, could be in violation of the regulation without ever knowing or having an opportunity to directly request guidance from the Secretary; and

(2) State governments could have a conflict of interest, as one of the largest health data collectors, in bringing forward queries to the Secretary.

Compliance and Enforcement

Due to the lack of concrete guidance in its current form, the proposed regulation may unwittingly expose physicians and other covered entities to fines for noncompliance despite good faith efforts to comply. The AMA is also troubled by the implicit federal overlap created by this rule wherein the traditional role of the states' medical licensure boards in overseeing physicians' ethical practice is usurped by federal enforcement.

We are encouraged to note the Secretary's philosophy of providing "a cooperative approach to obtaining compliance," that looks to an educational, rather than punitive, approach to resolve disputes. The AMA nevertheless questions the role of the Secretary or any federal officer to investigate complaints against physicians for breaches of patient confidentiality. This is the traditional realm of state medical licensing boards and their premier role in pursuing this type of activity is clearly articulated in State medical practice acts.

Cost of Compliance

The AMA notes that the cost to comply with the proposed privacy regulations clearly is not a one-time cost but will be a perpetual and continuing commitment, and this should be reflected in the analysis. These continuing costs are not anticipated by the proposed rule. Furthermore, the proposed rule could impose significant new costs on physicians' practices, with the potential to disproportionately burden small physician offices. We believe this runs counter to the explicit intent of HIPAA's "Administrative Simplification" provisions, which require "any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care." (Sec. 262. "Administrative Simplification," "Sec. 1172(b) Reduction of Costs.")

Conclusion

The Secretary notes that she has attempted to create a regulation that strikes a balance between permitting important uses of health information while respecting an individual's right to privacy. We commend the Secretary for the attempt to address these complex issues, particularly within the restrictive framework permitted under HIPAA. The AMA does not believe, however, that the proposed regulation achieves the necessary and proper balance. The proposed regulation would not adequately protect patient privacy and confidentiality and it would substantially and unacceptably increase administrative burdens for physicians. For these reasons, we cannot support the proposed regulation in its current form.

Further, the parameters set under HIPAA for regulatory action do not permit the full scope of protections that physicians believe patients deserve in any federal privacy law. We believe that the first step of any ultimately successful proposal, legislative or regulatory, must be to place the patient first. Each entity seeking access to patients' most confidential medical information must pass the stringent test of showing why its professed need should override individuals' most basic right in keeping their own information private. Moreover, citizens deserve a full and open discussion of exactly who wants their private medical information and for what purpose. Only then may the true balancing of interests take place. These are the ground rules of AMA policy and they should be the ground rules for the federal debate regarding patient privacy.

Chairman THOMAS. Thank you, very much, Doctor. Ms. Fox?

STATEMENT OF ALISSA FOX, EXECUTIVE DIRECTOR, OFFICE OF POLICY AND REPRESENTATION, BLUE CROSS BLUE SHIELD ASSOCIATION

Ms. FOX. Mr. Chairman and members of the committee, thank you very much for this opportunity to speak to you today.

Blue Cross and Blue Shield Association agrees that standards are necessary to assure all consumers that their medical information is kept strictly confidential. For our plans, there is absolutely no question as to whether patient records should be kept private, but only as to how this should be done.

We have extensive reviewed the proposed HHS rules with our plans and have concluded that without substantial changes, the proposal is operationally infeasible, extremely costly, and would threaten quality improvement efforts throughout the health care system.

Today, we submitted over 50 pages of detailed formal comments, as well as recommendations to HHS. I would like to highlight our four top issues.

First, as discussed earlier, this proposal would layer new Federal rules on top of existing state laws that will make it extremely confusing for everyone. HLC has an excellent chart illustrating this.

For consumers, it will be extremely difficult to know what their rights are, and who do you call when you have questions or problems? Do you call the state? Which state? How many states? Or do you call HHS?

Second, the new business partner requirement would force plans, doctors, and hospitals to assure all of their partners comply with these rules. This is simply unworkable and would be very expensive because everyone would end up monitoring everyone else. Hospitals monitoring doctors, plans monitoring hospitals. We have urged HHS to drop this requirement.

Third, the new minimum necessary rule would require all of us to establish new procedures and reorganize and redesign our operations, so we are only disclosing the minimum information necessary in each and every case. This would undermine all of our efforts to assure that patients receive the right care at the right time.

Simply put, this erects road blocks to assuring patients receive the best possible care and runs counter to the new Institute of Medicine report, which highlights the need for complete and timely access to patient medical information to prevent the wrong care.

Fourth, we are concerned that the way the proposal is constructed, it may make it difficult and perhaps even impossible for plans to continue existing beneficial functions such as disease management programs. This is because the list of the functions in the health plan definition misses many key functions we do today. And we worry that it could limit what we do in the future as we evolve to meet consumer demands in the 21st century, where the pace of technological advances continues to amaze us all.

Finally, we are extremely concerned about the cost of implementing such a complicated proposal. We commissioned the Nolan Company to estimate the cost of several provisions and their estimate is over $40 billion for the entire health care system over a five year period. This estimate is multiple times higher than the HHS estimate.

A key reason for this difference is that HHS did not estimate many of the provisions we believe will be extremely expensive. HHS has said they did not have the information and data to do these estimates. We hope that our study will be useful to them.

Mr. Chairman and members of the committee, let me close by saying that we must be smart in what we ask of the health care system. We must evaluate new requirements very carefully to make sure that they are the most cost effective and efficient way of protecting patients. We believe that major changes are needed to assure we are not unnecessarily adding to the cost of insurance coverage or jeopardizing our health care system which continues to provide the best care in the world. And most importantly, we must avoid redirecting scarce dollars from benefits to administrative costs.

Thank you very much.

[The prepared statement follows:]

Statement of Alissa Fox, Executive Director, Office of Policy and Representation, Blue Cross Blue Shield Association

Mr. Chairman and Members of the Committee, I am Alissa Fox, Executive Director for the Blue Cross and Blue Shield Association. The Blue Cross and Blue Shield Association (BCBSA) represents 49 independent Blue Cross and Blue Shield Plans across the country, covering over 74 million Americans -or one in every four individuals.

Thank you for the opportunity to testify today regarding our major concerns with the proposed regulations setting privacy standards for individually identifiable health information issued by the Department of Health and Human Services (HHS) on November 3, 1999.

BCBSA believes that safeguarding the privacy of medical records is of paramount importance. All consumers should be confident their medical information is kept confidential. For BCBS Plans, there is no question as to whether patient records should be kept confidential, but only as to how this should be accomplished. We look forward to working with Congress and the Department of Health and Human Services (HHS) to implement practical privacy protections that:

- allow for the timely delivery of and payment for health care services;
- facilitate efforts to deliver safe and high quality care; and,
- minimize costs and administrative paperwork for consumers, providers and others in fulfillment of the objectives of Health Insurance Portability and Accountability Act's (HIPAA) Administrative Simplification provisions.

It is clear from the proposed regulation that HHS sought to balance the need to safeguard medical records with the ability of the health care system to provide health care services efficiently. We recognize that the staff of HHS has worked long hours in an attempt to develop regulations that would not impede our modern health care system.

However, despite their efforts, we remain concerned that the proposed regulation needs significant revision. Without substantial changes, the proposal is operationally infeasible and extremely costly. It would slow the delivery and payment of care to providers and consumers, threaten the assurance of quality, and exacerbate the cost of health care.

My testimony focuses on five key areas:

I. Scope of the Regulation
II. Key Concerns with the Regulation
III. Positive Aspects of the Regulation
IV. Cost of the Regulation
V. Recommendations

I. Scope of the Regulation

HIPAA provided HHS the authority to promulgate privacy standards for consumer health information if Congress did not pass legislation by August 1999. The statute directed HHS to issue rules governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a)''—certain standardized transactions for claims payment and other functions. This directs the Secretary to develop a narrow set of privacy rules for the specific transactions that are developed and transmitted under Administrative Simplification. However, the proposed rule establishes standards that far exceed this mandate. The proposal would affect virtually all players in the health care industry as well as many other organizations—such as schools, employers, and accounting firms -and the vast majority of information.

The proposal would require covered entities (i.e., health plans, providers, and clearinghouses) to:

- Obtain new authorizations from consumers before using or disclosing information, except for purposes of treatment, payment, health care operations and other limited circumstances;
- Allow individuals to inspect, copy and amend much of their medical information;
- Track all disclosures made other than for treatment, payment and health care operations;
- Recontract with all business partners to require them to use and disclose information according to the new privacy rules and assure that business partners are complying;
- Institute procedures to assure that only the minimum information necessary is used or disclosed for a given purpose;
- Designate a privacy official and train staff;
- Follow specific rules before using protected health information for research; and,
- Develop a host of new policies, procedures and notices.

In understanding the full scope and implications of the regulation, it is important to be aware of the following:

- *The Regulation is Not Limited to Electronic Records:* Many news accounts describe the proposed regulation as applying to electronic records only. This is far from accurate. The regulation specifically applies to electronic records, as well as any format of a record that has ever (or will ever be) electronically transmitted or maintained. This broad brush covers millions of paper records, oral records and other storage formats. In addition, because it would be so difficult to distinguish ordinary paper records from paper records that had been (or would be) electronically transmitted, the practical effect of the regulation would be that doctors, health plans and other covered entities would need to apply the protections to all of their records, of *any* format.
- *The Regulation Affects Internal Uses of Information as well as Disclosures:* A common misconception regarding the regulation is that it simply regulates the disclosure of information to a third party. In fact, the regulation actually affects the use of information internally within an organization. This means that organizations would be required to comply with all the rules even when they use information *internally* for treatment purposes, claims management, utilization review and other routine health care purposes.
- *The Regulation Affects a Broad Array of Organizations and Information:* The definition of ''covered entity'' in the regulation is broad in scope—including not only doctors, hospitals and health plans but employers operating their own health plans (insured/self-funded), laboratories, pharmacists and many others. Many organizations that are not included specifically as a ''covered entity'' are indirectly subjected to the privacy rule through a new requirement that all covered entities must regulate their ''business partners.'' For instance, lawyers, accountants and other non-health oriented organizations could fall into this category.
- In addition, the definition of ''protected health information'' (PHI) in the regulation is much broader than what most individuals consider their health information. The definition of PHI goes beyond an individual's medical records to include insurance records and status, oral information, demographic data, and insurance status.

II. Key Concerns with Regulation

Today, BCBSA submitted over 50 pages of detailed formal comments to HHS on a whole host of important operational issues. This testimony highlights the four most problematic provisions in the regulation.

1. Preemption of State Law

We believe doctors, health plans, and other covered entities will be unable to navigate the labyrinth of state and federal privacy laws under the complex construct of the HIPAA regulatory model. The regulation follows HIPAA regulatory construct in that state laws are preempted only if contrary to the regulation, and less stringent. In addition, the regulation specifically "saves" certain state statutes from preemption, such as those relating to health surveillance.

Everyone in the health care system needs a clear understanding of the rules that guarantee privacy. We are concerned that the lack of a complete preemption over state law creates a serious problem for consumers, doctors, health plans and other covered entities.

Doctors, health plans and other covered entities must determine, on a provision by provision basis, which parts of state law would be retained, and which would be replaced by federal law. This is further complicated by the free flow of patients and information in today's health care industry. For instance, an individual may live in the District of Columbia, work in Virginia, and visit a physician located in Maryland. Covered entities dealing with this individual must evaluate the interplay of three state statutes with the federal law. In addition, covered entities also must factor in the interplay of other federal laws relating to privacy. Even if each covered entity engaged an attorney to prepare a preemption analysis, different attorneys would prepare conflicting interpretations—leading to costly litigation with the states, the federal government and consumers.

This regulatory construct particularly will be confusing for consumers. Instead of facilitating an individual's ability to know their privacy rights, this complex preemption process is sure to confound patients. First, individuals will be hard pressed to determine which aspects of the state and federal privacy laws apply to them, so it will be impossible for them to determine if in fact, they have been wronged. In addition, consumers will not know where to direct complaints if they do feel that their rights are violated —Maryland? Virginia? The District of Columbia? The Secretary of Health and Human Services? It is likely that consumers will be bounced from one jurisdiction to the next until the consumer locates the one which has the law that has been violated -or the consumer becomes frustrated and terminates the effort.

We recognize that a complete preemption of state law is outside the statutory authority of the Department of Health and Human Services (HHS). Therefore, we recommend HHS prepare a detailed privacy guide for each state on how existing state laws intersect with the new federal rules. The guide should also address whether a privacy provision is triggered by a consumer's residence, location of provider or other criteria. HHS should prepare the guide in collaboration with state government officials. HHS should assure this guide also incorporates other federal privacy laws, such as the Federal Privacy Act. As part of this process, each individual state should certify agreement with HHS' analysis so everyone has a clear understanding of the rules.

It is imperative that this legal guidebook is prepared well in advance of the final regulations. Doctors, health plans, and other covered entities will need this completed analysis before computer systems can be redesigned, forms and notices are changed, consumer brochures are modified and updated, and other procedures can be brought into compliance. Bringing plan and provider operations into compliance with these complex new regulations will be expensive, so it is critical that these entities only have to modify systems and other items once. Therefore, we recommend that the analysis be provided two years prior to the effective date of the regulation.

2. Business Partners

The business partner provisions of the regulation require that doctors, health plans and other covered entities enter into prescribed contracts with all of their "business partners" to assure these partners follow specific HHS privacy rules. The doctors, health plans and other covered entities would be considered to be in noncompliance with the regulations and could be subject to penalties and/or litigation if they "knew or reasonably should have known" of certain privacy violations of their business partners. We believe these provisions are unworkable, as well as outside of the authority of HHS.

The definition of business partner is so broad that physicians could be the business partners of independent laboratories; health plans could be the business partners of their lawyers and accountants; and hospitals could be the business partners of independent physicians that practice within their walls. Doctors, hospitals, Coordination of Benefit (COB) partners, and health plans could all be construed as "business partners" of each other. These provisions also could result in unworkable relationships between government agencies. For instance, we believe the Social Se-

curity Administration—who makes eligibility determinations for the Medicare program—could be interpreted to be a business partner of the Health Care Financing Administration (HCFA). Medicare contractors could be business partners of HCFA, subjecting HCFA to the fines and penalties under the regulation.

The potential liability is likely to force all of these doctors, health plans, and other covered entities to monitor each other (as well as sub-contractors). This would result in an enormous amount of duplicative monitoring and auditing, making it likely that all members of the health care industry would be monitoring each other (including covered entities)—an obvious conflict with the efficiency and cost-saving goals of the Administrative Simplification provisions of HIPAA. Moreover, these costly actions would provide little or no real benefit to consumers since most of these entities already would be covered by the regulations.

The contractual specifications included in the regulation compound the problems in the unworkable business partner framework. For instance, one of the specified contract standards in the regulation is that doctors, health plans, and other covered entities require business partners to either destroy or return all protected health information (PHI) when a contract is terminated. But clearinghouses, for example, keep health data on file for some time to respond to disputes and complaints. Health plans, employers, and other covered entities and business partners must maintain PHI in order to provide HIPAA certificates of coverage and protect themselves from legal disputes, complaints, etc. In addition, some health plans are required by state law to keep information for a certain period of years for state purposes. This is only one of a number of examples demonstrating the operational infeasibility of the contract provisions. In our detailed comments, we identified a number of other.

And finally, we believe the business partner provisions are outside of the statutory authority of the Department of Health and Human Services. HIPAA clearly delineates the covered entities subject to HHS oversight: health plans, clearinghouses, and providers conducting standard transactions. Attempts to indirectly regulate other organizations—through doctors, health plans and other covered entities or otherwise—is an overreach of regulatory authority. We believe recent District and Supreme Court cases support this premise as well as the viewpoint that inherently federal powers cannot be delegated to non-federal authorities.

3. Minimum Necessary

The proposed regulation instructs doctors, health plans, and other covered entities to use or disclose only the minimum information necessary to accomplish a given purpose and discourages the exchange of the entire medical record. This requirement also implies determinations should be made on an individual basis. At first blush, this standard seems to be a perfectly reasonable, common sense provision.

However, upon an operational implementation perspective, it becomes increasingly clear that it would be impossible to implement a legal standard that only the minimum information is used or disclosed. First of all, it is important to recognize that this standard applies to the use of information as well as disclosure, and that the definition of disclosure includes broad terms such as "provision of access to." We believe this standard would require a massive reorganization of workflow, as well as possible redesign of physical office space and would jeopardize the quality and timeliness of patient care, benefit determinations and other critical elements of the health care system. For instance:

- As part of the description regarding the minimum necessary standard, the regulation includes a strong discouragement regarding the release of entire medical records of patients. The complete exchange of medical information is absolutely critical to assuring a patient receives the right treatment at the right time. The recent Institute of Medicine report, "To Err is Human," highlighted the medical mistakes that are common in our health care system today. The IOM report states that errors are more likely to occur when providers do not have timely access to complete patient information. The discouragement of complete medical records would make it more difficult to guard against these problems. One covered entity may determine that a subscriber's prescription is not relevant to be released. Further down the line, that lack of information may impede clinicians' decisionmaking.
- It is well documented that fraud and abuse is a costly element of our health care system. The Medicare program as well as private health plans have made combating fraud and abuse a priority. However, the minimum necessary standard is likely to impede fraud detection, because fraud and abuse units may be accused of using more than the minimum information necessary. Any impediment to fraud detection would increase the cost to consumers.
- Health plans and providers actually may be forced to redesign their facilities to comply with the minimum necessary standard. For instance, when visiting friends in maternity wards, there generally is a white board describing all of the

patients and their medical needs. Any visitor may view the information on the board. Or take an orthopedist's office, where a x-ray lightboard is centrally located outside of the patients' rooms for easy access by the physician. Anyone in the office could view the x-rays, and x-rays are identifiable information. Would the regulation require these providers to renovate their facilities to comply with the regulation?

These are a few examples of the types of activities that could fall awry of the proposed privacy regulations. If implemented, this would impose incredible costs on consumers—not just in dollars and cents—but in lives as well.

4. Health Care Operations

One of the fundamental building blocks of the regulation is its definition of health care operations. Items that are listed in this definition are exempt from the requirement to track disclosures of protected health information, and do not require a separate authorization from an individual. As changes are made to the final regulation, we expect the definition to continue to play a key role.

We believe the current definition of health care operations misses important functions. As a result, covered entities may have to solicit authorizations for certain functions or track disclosures as part of routine operations. The end result would be that health plans could encounter major obstacles to conducting these activities and could be discouraged from conducting these important functions. The following is a sample of overlooked functions:

- *Disease management, case management, risk assessment, epidemiological studies and drug interventions.* Many of our Plans conduct these important programs that benefit consumers through improved health care, better outcomes, and lower cost. For instance, the Blue Cross and Blue Shield Federal Employee Program provides disease management services to improve care for patients with respect to congestive heart failure and diabetes as part of its benefit plans. When claims are processed, the names of enrollees that could benefit from disease or case management are compiled. This information also may be used to conduct epidemiological studies of particular populations within FEP or to implement drug intervention programs.
- *Private accreditation by organizations such as National Committee for Quality Assurance (NCQA), as well as auditing, evaluating and accreditation functions performed by other private entities, such as associations.* The NCQA and other private accrediting organizations sometimes require the review of information that could be considered as protected health information. In addition, other private entities—such as associations—sometimes perform auditing and evaluation of their members as part of membership or other standards.
- *Routine Plan operations such as "security activities," data processing activities and general maintenance:* Some health plans conduct a series of security activities designed to assure that employees are complying with corporate privacy policies. For instance, they may monitor "same name" look-ups, to guard against employees checking the records of family members, or monitor access to celebrity files, as well as other initiatives. With regards to computers, "live" data is often used in order to assure that system changes and upgrades have correctly been made. Health Plans also must conduct a number of routine operations, for instance the printing of ID cards, etc.
- *Health promotion and other educational activities.* For instance, FEP has established a 24-hour nurse hotline, Blue Health Connection. Enrollees' PHI may be disclosed to the vendor responsible for Blue Health. This information is used to provide enrollees with health education, treatment options, and assistance with questions for enrollees to ask their physicians. We also may notify enrollees -or require our physicians to notify patients—regarding mammography screenings or immunizations.
- *Insurance underwriting and other activities:* While the regulation does specify insurance underwriting, we believe the proposed definition may be deficient because it relates only to the renewal of a contract, and to the protected health information of individuals already enrolled. This could inhibit our ability to develop an appropriate premium for group coverage as well as the ability of covered entities to obtain stop-loss coverage or reinsurance.

This is only a sample of the types of functions that have been overlooked. We believe many more items will be discovered as doctors, health plans, and other covered entities begin implementing the regulation. In addition, we believe the definition is static, and cannot reflect the new roles and functions that health plans may develop in the future that benefit consumers, improve quality, and reduce costs. For instance, if this definition had been developed ten years ago, disease management programs would not be as common as they are today. We are concerned that such strict definitions could limit health plans' roles as they seek to redefine themselves to meet consumer demands of the 21st century. We believe a static definition of health

care operations will squelch innovation because health plans will not invest in development unless they know the new program would fall under health care operations.

III. Positive Aspects of the Proposed Regulation

Clearly, we believe there are significant issues in the proposed regulations. However, the regulations did include certain provisions that demonstrated interest in balancing operational impacts with the overall goal of privacy. We have urged HHS to retain these provisions in the final regulation. In particular:

- *"Statutory" Authorization for Treatment, Payment and Health Care Operations:* The proposed regulation does *not* require a new authorization for treatment, payment, and health care operations. We believe a "statutory" authorization, meaning that covered entities may use or disclose protected health information (PHI) without authorization as matter of law, is imperative and would oppose a requirement for new authorizations for these vital activities.

Requiring health plans to obtain a new authorization from current subscribers would require numerous mailings and phone calls from health plans—a process akin to a "late bill" collections process—in order to obtain the new authorizations. In the interim, subscribers and providers would experience delays in payment and other services and confusion in the health care system.

- *Tracking of Disclosures, Other Than For Treatment, Payment and Health Care Operations:* The proposed regulation requires tracking of disclosures made for purposes *other than* treatment, payment or health care operations. This requirement is operationally more feasible than a requirement to track *all* disclosures. We would oppose *any* expansion of this standard. Expanding the tracking standards would result in duplicative and unnecessary tracking of millions of routine transactions that occur every day (e.g., Coordination of Benefits, lab disclosures to physicians, etc.) and a blizzard of paperwork for all, especially physicians. However, we remain concerned that this more reasonable tracking standard is undermined by provisions in the amendment and correction standard that requires doctors, health plans and other covered entities to notify previous recipients of information. If the amendment and correction standard is not modified, we believe it would have the operational effect of a "de facto" tracking standard for all disclosures, even those made for treatment, payment, and health care operations.
- *Inspection And Copying Of PHI Contained In A Designated Record Set:* The proposed regulation allows consumers to inspect and copy those records retrieved from a designated record set used to make substantive decisions. Using a designated record set standard is operationally more feasible than requiring access to all protected health information. Expansion of this standard to all records would result in reams of meaningless information being retrieved and copied at a great cost to the health care system. We oppose expansion of the current standard.

VI. The Cost of the Regulation

The proposed regulation includes an estimated total cost of $3.8 billion over five years. We think this figure greatly underestimates the cost of implementation. The regulation itself indicates the HHS cost estimates are incomplete. The proposed regulation itemizes 10 standards for which HHS was unable to complete a cost analysis, noting that "the cost of these provisions may be significant in some cases. . .." The minimum necessary standard, business partner monitoring, designation of privacy officials and privacy boards, and creation of de-identified information were all items excluded from the HHS cost estimate.

Due to our concern regarding costs, we engaged the Robert E. Nolan Management Consulting Company to provide an independent estimate of several key provisions of the proposed regulation; the Nolan estimate is over $40 billion over five years to health plans, providers and other members of the health care community. These costs stem from:

- *Business Partner Monitoring:* The business partner provisions would make doctors, health plans and other covered entities liable for the compliance of their business partners, including lawyers, schools and other organizations. As a result, covered entities would monitor each other as well as their non-health business partners. This provision is estimated to cost about $4 billion over five years.
- *Privacy Officials, System Changes and other Infrastructure:* Doctors, health plans and other covered entities would need to retrain current employees and periodically recertify their employees, hire privacy officials, upgrade systems, and address other infrastructure issues in order to implement the proposed privacy regulations. This is estimated to cost about $23 billion over five years.
- *Tracking and Disclosure:* The amendment and correction provision requires covered entities to send amended records to previous recipients of the information. This

could result in a "de facto" requirement to track all disclosures of information. As a result, this provision could cost as much as $9 billion over five years.

- *Inspection, Copying and Amendment:* Covered entities would have to allow individuals to inspect, copy and amend all information contained in a designated record set. The definition of accessible information extends beyond the traditional medical record to other electronic, or written information that includes an individual's name, social security number or other identifying feature. This provision is estimated to cost almost $4 billion over five years.
- *Impact on Medical Management:* Deficiencies in the term health care operations and other definitions could reduce the ability of health plans to conduct effective disease management programs. These programs improve the quality of care of consumers, and decrease overall medical costs. Less effective disease management programs is estimated to cost $3 billion over five years.

Obviously, estimates will vary depending on the final interpretations of the regulation, however we believe an estimate of over $40 billion remains conservative. For instance, it does not include the new liability costs that will arise from this regulation, the impact of underwriting changes, or the impact on health research. Ultimately, the additional administrative costs faced by providers and health plans will increase the cost of insurance coverage.

V. Recommendations

In general, the proposed regulation require doctors, health plans and other covered entities to implement complex new rules that require extensive new procedures, documentation processes, form specifications and notice standards. These requirements would require the re-organization of workflows as well as possibly the physical facilities of doctors and hospitals in order to comply with the law. We believe the level of documentation and procedures is unnecessarily excessive, and should be rewritten to reduce the complexity, burden and cost.

Specifically, we urge the following:

(1) Detailed Guidance on Preemption of State Law: While we recommend a full preemption of state law in the privacy area, we understand that it is outside of the statutory authority for HHS. In the absence of full preemption, we recommend HHS, working with the states, prepare a detailed analysis of state and federal law to provide a clear guide on all provisions affecting the health care industry.

It is critical that this guidance is available at least two years prior to the effective date of the regulation. Bringing operations into compliance with these complex new regulations will be expensive so it is critical that doctors, health plans, and other covered entities only have to modify systems and other items once.

(2) Removal of Business Partner Provisions. The business partner provisions should be removed from the regulation because they are:

- Outside of the Secretary's statutory authority
- Unworkable and would create expensive and duplicative monitoring between doctors, health plans, and other covered entities
- Unnecessary since the vast majority of protected health information is maintained by organizations that are covered by the regulation.

(3) *Change the Minimum Necessary Standard from Legal Standard to Organizational Objective:* While we believe the minimum necessary standard is a laudable goal, we are concerned that it would be impossible to implement this standard operationally and comply with a rigid legal standard. Therefore, we recommend that organizations include the minimum necessary standard concept as an objective, rather than as a legal standard.

(4) Revise Definition of Health Care Operations: The current definition of health care operations is static and missing key elements. As the building block of the regulation, this definition is crucial because it triggers whether or not new authorizations are required, disclosures are tracked, and other important issues. Instead of using a narrow, prescriptive definition, we recommend inclusion of a definition that is flexible enough to incorporate the industry's current operations as well as new ones that develop as our ability to improve quality and other areas increase.

(5) Additional Funding for Medicare Contractors and other Government Programs. We also urge congressional appropriators to factor the additional cost of privacy compliance into budget development regarding the Medicare fee for service contractors, Medicare+Choice plans, the Federal Employees Health Benefit Program, and other federal programs.

VI. Conclusion

Once again, we appreciate the opportunity to testify before you on this critical issue.

We would like to continue working with you, and the Department of Health and Human Services, on crafting privacy rules that meet our common goals of protecting consumers, improving quality, and minimizing costs.

Thank you again for this opportunity to testify on this important issue.

Chairman THOMAS. Thank you, Ms. Fox. Ms. Goldman?

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

Ms. GOLDMAN. Good morning, Mr. Chairman, Mr. McDermott, members of the subcommittee, thank you very much for testifying today.

The Health Privacy Project at Georgetown was created a number of years ago to look at the impact of privacy in the health care setting. We have since participated in and there has since been numerous polls and surveys that have shown that the lack of privacy in health care has been a major barrier to people seeking care and to the quality of care that people receive.

Congress, of course, acknowledged that concern and, in the Health Insurance Portability and Accountability Act, you imposed a deadline on yourselves to address this issue in a comprehensive way. Of course, after many bills were introduced and many hearings, many of which were held by this subcommittee, the deadline did pass and that then triggered the requirement on the administration to issue regulations.

They did extend the comment period based on our request and a number of requests of those sitting here at this table, so that we had a full chance to put our comments in. That comment period closes today. This hearing is important because it gives us again another opportunity, while we are still in the draft stage, to make sure that this is as strong and workable a regulation as possible.

What I want to focus on in my testimony are two areas. One, there are gaps in the Secretary's proposed regulation that are there because of the legal constraints on her delegation of authority from HIPAA. The second is to just go through quickly the strengths and weaknesses in the proposed regulation itself.

There are three major gaps in the regulation, again stemming from the delegation of authority in HIPAA. They have already been covered, but let me please go through them quickly. The issue of electronic versus paper records. We think it is really senseless to have a rule that only applies to electronic records, because it goes against the intention in HIPAA which is to create a uniform standard electronic network. And you do not want to create a disincentive for people to put information into electronic form as a way of avoiding the privacy regulations.

The second is the issue of covered entities. Some of the concerns that many of my colleagues have about how the regulation is drafted is based on the fact that the administration can only cover three entities directly, the plans, the providers, and the clearing houses.

So the scope of coverage through the business partners language and through other prohibitions on disclosure is in there as a way of making this a workable regulation. And it is there because the screening is limited in what she is able to do in terms of scope. So I think that is an important issue to look at.

The third gap obviously is on enforcement. We are very concerned about the weak enforcement and the weak remedies that are available under the proposed regulation. Again, HHS was constrained because of HIPAA.

We do think though that, on balance, the regulation is vitally important as an intermediary step and I say that recognizing that Congress still has a very important role to play in both filling the gaps and strengthening certain provisions. We look forward to working with you on that. I think the regulation will set a baseline of protection, but we need to look at some of the major provisions that are being proposed.

One, it gives people the right to see their own records, a critical right, one that is not uniformly and comprehensively provided for at the state level. The regulation itself creates an overall incentive to use de-identified data. Again, if you create de-identified data, you are outside the scope of the regulation. It provides notice to patients about how their information will be used and by whom. It provides for an authorization process.

We are very concerned, however, that in that first tier of authorizations, for treatment, payment, and health care operations, the lack of any opportunity for individuals to sign a form either saying "I understand how my data is going to be used", or "I am authorizing the use of that data"—which is essentially what the status quo is. We are very concerned that people will not truly understand how their information is flowing.

While the business partners proposal, is awkward in many ways, it is a necessary way of creating a chain of trust in how information flows and to whom. In many ways, it is codifying what is already good business practice. You clearly do not disclose information to agents or others without entering into a written agreement about how that information will be used.

On research, we are very pleased to see the Secretary's proposal to expand either the institutional review board structure or a privacy board to cover all research. However, we would like to see it be an institutional review board.

On law enforcement, I think she has fallen short of where the regulation needs to be. It appears to be an improvement over the initial recommendation, but it allows for a kind of—excuse the cliche—a Chinese menu of choices in determining what kind of legal process law enforcement needs to get. We think that must be strengthened.

On remedies, again a private right of action is necessary to make this an effective provision. Clearly that is an important area for Congress to explore. All other Federal privacy laws include a private right of action.

On preemption, I want to address some of the comments that my colleagues have made about preemption. We did a survey of state confidentiality laws to look at what was the state of health privacy right now. What we have found is that if you read the regulation

that is being proposed, you will create significant uniformity in how health privacy is handled at the state level, because many of the laws are weaker than what is being proposed by the Secretary at this stage. And where they are more detailed and more protective are in, for the most part, condition specific areas, where the states have gone to great pains to enact detailed specific provisions dealing with HIV, with mental health, with reporting, with abuse and neglect.

And so our state report essentially shows you will have substantial uniformity with the passage of a Federal law, even one that sets a floor. It will make the operation of the health care system much more efficient, more cost effective and, I think, more fair.

In conclusion, Congress set the wheels in motion for where we are today with the Secretary's proposal. I think it was an important trigger mechanism so that we would have something, again as an intermediary step.

This has been a tough issue for Congress. There are lots of different interests. It has been hard to find consensus. But in fulfilling the legal duty imposed under HIPAA, the Secretary has proposed some regulations that will take us part of the way.

What we urge is for Congress to take us the rest of the way, to finish the job, and to fill the gaps and to strengthen the weaknesses. In the meantime, we hope that the proposed regulation will be strengthened, that the Secretary will have an opportunity to respond to many of the concerns that we have all raised, and that you have raised this morning, and that the regulation should go forward.

Thank you very much.

[The prepared statement follows:]

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

I. INTRODUCTION AND OVERVIEW

Mr. Chairman and Members of the House Subcommittee on Health of the Committee on Ways and Means: I very much appreciate the invitation to testify before you today on the Administration's proposed regulations regarding the privacy of individually identifiable health information.

In December 1997, I launched the Health Privacy Project at the Institute for Health Care Research and Policy and Georgetown University Medical Center. The Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level.

Congress recognized the importance of protecting health privacy when it passed the Health Information Portability and Accountability Act of 1996. HIPAA requires that if Congress failed to pass comprehensive health privacy legislation by August 21, 1999, the Secretary of Health and Human Services must issue regulations by February 21, 2000.

Congress did in fact fail to meet the August deadline. Consistent with its legal duty under HIPAA, the Administration did issue draft health privacy regulations November 2, 1999. The comment period was extended to February 17, 2000. We expect the regulations to be finalized in April.

The proposed federal health privacy regulations constitute a significant step towards restoring the public trust and confidence in our nation's health care. These rules, however, are by no means the final solution. By virtue of the limited authority delegated by Congress, the proposed rules have limited applicability and cover only health plans, health care clearinghouses and health care providers who transmit health information (";covered entities") in electronic form. We appreciate the fact that the Secretary has made a strong effort to extend this coverage to a covered entity's business partners. But a large segment of those who hold health information remains beyond the scope of these regulations.

Our testimony today focuses on two areas: 1) the limitations of the Secretary's authority and the role Congress should play to strengthen the final rule and fill remaining gaps in protection, and 2) the strengths and weaknesses of the proposed regulation.

II. PUBLIC NEED AND DEMAND FOR HEALTH PRIVACY

A substantial barrier to improving the quality of care and access to care in this country has been the absence of enforceable privacy rules. People are withdrawing from full participation in their own health care because they are afraid their health records will fall into the wrong hands, and lead to discrimination, loss of benefits, stigma, and unwanted exposure. A January 1999 survey by the California Health Care Foundation found that one out of every six people engages in some form of privacy-protective behavior to shield themselves from the misuse of their health information, including lying to their doctors, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and—in the worst cases—avoiding care altogether. (Survey released by the California HealthCare Foundation, January 1999)

Without trust that the personal, sensitive information they share with their doctors will be handled with some degree of confidentiality, people will not fully participate in their own health care. As a result, they risk inadequate care or undetected and untreated health conditions. In turn, the integrity of research and public health initiatives that rely on complete and accurate patient data may also be compromised. Thus, protecting privacy and promoting health care quality and access are values that must go hand-in-hand.

III. THE ROLE CONGRESS SHOULD PLAY

The Secretary's authority to promulgate health privacy regulations is delegated to her in the Health Insurance Portability and Accountability Act. Due to the constraints imposed on her authority by HIPAA, the practical impact is that the draft regulation falls short in terms of scope of coverage and enforcement. Congress should act swiftly to fill these gaps to ensure that Americans have strong and comprehensive health privacy protections.

A. Who is Covered: Scope Should be Expanded

The draft rules issued by HHS only apply to certain entities: health care providers, health plans, and clearinghouses (entities that process and transmit claims data). We recognize that the scope of entities covered by the regulations is limited by the terms of HIPAA, and that the Secretary has attempted to cover as many entities as possible given her limited delegated authority. By limiting the regulations to health plans, health care clearinghouses, and certain health care providers, however, Congress has left a large number of entities unregulated, leaving gaps in the protection afforded health information. Many providers, researchers, and oversight agencies, for example, will not be subject to this regulation even though they collect, use, and disclose protected health information that identifies individuals.

The Secretary has chosen to bind some non-covered entities to the principles of the draft regulation by requiring covered entities to establish contracts with business partners, or by prohibiting disclosures. This is a good intermediary step to fulfill the intention of the privacy language of HIPAA. However, this approach has significant limits, including the liability borne by covered entities, and the difficulty in prohibiting re-disclosure by non-covered entities.

The only way to eliminate these gaps is for Congress to enact a comprehensive health privacy law. We therefore strongly urge Congress to pass a comprehensive health privacy law applicable to all those who generate, maintain, or receive protected health information.

B. What is Covered: Paper Records Should be Protected

The draft regulations only apply to electronic health information, but the vast majority of health information is currently maintained in paper form. We believe that the Secretary has the authority to extend the regulations that apply to all health information—whether it is maintained in paper or electronic format—and we recommend that she does so.

In the event that the final regulations do not cover paper records, we believe that it is appropriate and necessary for Congress to extend the protections to cover all records maintained or transmitted by covered entities.

The vast majority of health information is currently maintained in paper form. As proposed, the regulations distinguish between health information that at some point has been electronically maintained or transmitted and that which has not. This distinction is nonsensical, unworkable and unenforceable. At some point, some,

but not all, of the information in the record may be transmitted electronically. Under the current proposal, the paper record would then contain both protected information (i.e., information that has been electronically transmitted), and unprotected information (information which has not been so transmitted). It would be burdensome and difficult to identify and designate which information in any particular record is protected.

It would be easier for a covered entity to treat all information it maintains or transmits in the same fashion. Additionally, for enforcement purposes, it may prove difficult, if not impossible, to establish that specific health information at some point in its existence has been transmitted or maintained electronically and, therefore, is subject to the regulations. The best way to reduce these implementation and enforcement ambiguities is to make the privacy standards applicable to all individually identifiable health information transmitted or maintained by a covered entity regardless of its form.

Finally, the administrative simplification provisions of HIPAA appear to encourage the development of a uniform computer-based health information system. This goal is impeded by allowing paper records to remain beyond the scope of the regulations. There is little incentive for covered entities to convert to computer-based health information systems if they may avoid regulation by maintaining paper-based systems.

C. Enforcement: Private Right of Action Needed

Under HIPAA, the Secretary is unable to confer on individuals a private right of action in the event the rules are violated. When finalized, the regulation will be difficult for HHS to oversee and enforce, and no federal remedy will be available to individuals. Only Congress can fill these significant gaps.

In every other federal law that protects the privacy of peoples' records—from the Right to Financial Privacy Act to the Video Privacy Protection Act—Congress has seen fit to give people the legal right to go to court to seek injunctive relief and damages when the law has been violated. The remedies available under the proposed regulation are inadequate to ensure that the law will be fully, and forcefully, enforced. In the absence of a set of meaningful remedies, a real danger exists that compliance will be weak and spotty. While we understand the recent concern over lawsuits, we are unaware of significant problems that have resulted from the remedies now available to people under existing federal privacy statutes.

IV. STRENGTHS AND WEAKNESSES OF THE PROPOSED REGULATION

The following is a summary of the major provisions of the proposed regulation, with our comments. The Health Privacy Project also staffs the Consumer Coalition for Health Privacy, whose mission is to educate and empower healthcare consumers to have a prominent and informed voice on health privacy issues at the federal, state, and local levels. (A copy of the principles, Steering Committee, and endorsing organizations is attached. Information is also available at http://www.healthprivacy.org.) Members of the coalition are committed to the development and enactment of public policies and private standards that guarantee the confidentiality of personal health information and promote both access to high quality care and the continued viability of medical research. Funding for the Consumer Coalition is provided solely by the Open Society Institute. Many members of the Coalition are planning to submit their own comments on the draft Regulation. Others have endorsed the comments submitted by the Health Privacy Project and are reflected in the comments themselves.

The full text of our comments, with the names of endorsing organizations, is attached. (The comments are also available at http://www.healthprivacy.org.)

A. Who is Covered

Again, by statute, the Secretary can directly regulate only health care providers, health plans and health care clearinghouses, all of which are defined as "covered entities." We believe that the most effective way to extend the scope of coverage is through a comprehensive health privacy law that covers all entities that use and disclose individually identifiable health information.

In the draft regulation, the Secretary attempts to address this statutory weakness by requiring covered entities to have contracts restricting uses and disclosures with their "business partners," i.e., certain persons and organizations to whom they disclose protected health information. We commend the Secretary on her efforts to encompass as broad a field as possible under the proposed regulations. In our complete comments, we suggest ways in which the contracts between business partners might be improved.

The Secretary also attempts to address the circumstance under which an organization provides some health care or has created a health plan, but is not primarily engaged in these activities (such as a school that has an infirmary). Although the Secretary discusses treating only the health care component as a "covered entity," the regulations do not expressly carry out this intent. We suggest that this intent to designate only the health care component of a mixed entity as a "covered entity" be incorporated in the regulations. Additionally, the Secretary's explanation concerning employers and how they fit into the regulatory scheme is somewhat confusing. We suggest that the Secretary clarify the responsibilities of employers that sponsor health plans.

B. What is Covered

Again, the draft regulation currently only applies to health information maintained and transmitted in electronic form. We believe that the Secretary currently has the authority to promulgate regulations that apply to all health information—whether it is maintained in electronic or paper format—used and disclosed by covered entities.

C. Patients' Access to their Own Health Records

The draft regulations give people the right to see and copy their own health information, and to request that it be corrected or amended. We commend this effort to extend these fair information practices to health information.

We believe, however, that the Secretary has used a somewhat minimalist approach towards these rights. In our comments, we suggest a number of ways in which the right of access can be made more meaningful. Our major suggestions include:

- The decision to deny an individual's request for access to his health information should ultimately be made by a health care provider who is qualified to treat the patient for the condition that is the subject of the health information;
- There should be a meaningful appeals process for denials of access to health information; and
- The regulations should expressly state that a covered provider may not deny an individual access to his protected health information because of an unpaid bill for health care services.

D. Notice of Information Practices

The regulations give individuals the right to receive adequate notice of the information practices of covered plans and providers. We approve of this approach. We are also pleased that the regulation requires the notice to address the entity's existing information practices, rather than possible information practices, and suggest that this component of the regulation be preserved. We recommend changes that strengthen the notice provisions, including a requirement that covered entities make a reasonable effort to obtain a signed acknowledgment that the individual has received and read the notice of information practices.

E. Patient Authorization

The proposed rules would allow health information to be used and shared easily for treatment, payment and health care operations, without the consent of the patient. While we understand the need to strike a balance between individuals' privacy rights and the practical necessity of using and disclosing health information for certain purposes, we believe that the proposed regulations give too little weight to individual rights. Under the proposed rules, people have no ability to control or even monitor the use and disclosure of protected health information for purposes of treatment, payment and health care operations. We find this particularly disturbing given the Secretary's proposed construction that "treatment" includes the treatment of all individuals, not just the individual subject of the information.

- The regulations should require authorization from the individual for the use and disclosure of information for treatment, payment and health care operations, which should be renewed at least once every three years or whenever the patient changes insurance companies, whichever occurs first. At an absolute minimum, covered entities should have the option to require patient authorization for treatment, payment and health care operations.
- The terms "treatment" and "payment" should be narrowly interpreted as applying to the individual who is the subject of the information.
- The definition of "treatment" should be amended to ensure that disease management programs are only conducted with the authorization of the treating physician.

- The regulation should expressly state that the term "health care operations" includes only disclosures made to the covered entity (or a business partner of such entity) on whose behalf the operation is being performed.
- The regulations should limit the definition of health care operations to include only those operations that cannot be carried on with reasonable effectiveness and efficiency without protected health information.
- Health care providers should be subject to the verification requirements of the regulations when the request for information for treatment purposes originates outside of the covered entity.

We support the regulations' requirement that covered entities obtain an authorization from the individual for most uses and disclosures that are not directly related to treatment, payment or health care operations. We also strongly agree that consent must be voluntary, and cannot be tied to the delivery of any benefits or services. In addition to these requirements, we recommend that covered entities be required to obtain individual authorization prior to making certain disclosures of information pertaining to an individual's request or receipt of sensitive health services.

F. Minimum Necessary

The proposed regulation requires organizations to "make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure." We believe that this is the proper approach but that it does not go far enough because it does not apply to a large number of uses and disclosures. We urge the Secretary to extend this minimization requirement to most uses and disclosures.

G. Patient's Right to Restrict Disclosures

The proposed regulations give an individual the right to request restrictions on the use and disclosure of protected health information for purposes of treatment, payment, and health care operations. That request can only be made to a health care provider, and it must be agreed to by that provider. We suggest that the regulations be amended in the following ways:

- Allow individuals to have a true right to restrict (not just the right to request restrictions on) the use and disclosure of their protected health information where the disclosure of that information could jeopardize the safety of the individual.
- Allow individuals who pay for their own medical care (self-pay) to have a true right to restrict the disclosure of their protected health information.
- Allow individuals to require or request restrictions from all covered entities, not just health care providers.
- Require all covered entities that receive health care information that are subject to a restriction to comply with the restriction.

H. Psychotherapy Notes

We strongly commend the Secretary for excepting psychotherapy notes from the general rule allowing for the free flow of information for treatment, payment and health care operations purposes. The proposed regulations limit access to psychotherapy notes, absent specific consent from the individual. We believe, however, additional protections are critical for ensuring the level of privacy essential for effective mental health care.

I. Law Enforcement

While we acknowledge the positive shift in the Secretary's approach from her 1997 position that law enforcement should continue to have unfettered access to medical records, this current proposal continues to fall far short of meaningful standards. We urge that the final regulation:

- Require that law enforcement officials obtain legal process issued by a neutral magistrate, and
- Require that legal process issue only after the magistrate has applied a strong legal standard in weighing the request.

J. Health Oversight

We believe it is critical for the Secretary to clearly distinguish between law enforcement access and access to conduct health oversight activities.

We are also deeply concerned that the health oversight section contains too few limits on access and reuse of protected health information. In particular, we believe that where health information is used in a health oversight investigation, there should be a prohibition on the re-use and re-disclosure of protected health information in actions against individuals. Such a limit is essential to ensure that the rel-

atively easy access afforded to health oversight officials does not become the back-door for law enforcement access.

While this prohibition may be beyond the Secretary's authority in this regulation, we do believe that the Executive Branch is empowered to issue an Executive Order barring the re-use and re-disclosure of protected health information obtained pursuant to oversight. Such an order would establish legally enforceable limits directly on the federal employees charged with executing health oversight responsibilities.

K. Research

We support the general approach towards research in the regulations. We are pleased that the regulation aims to establish uniform rules for researchers regardless of the source of funding. The regulation seeks to accomplish this goal, however, by allowing covered entities to disclose protected health information to researchers without patient authorization if the disclosure has been approved by an Institutional Review Board (IRB), or a newly created privacy board. We believe that the Secretary should eliminate the option of using a privacy board.

If the regulation does not bring all research under the Common Rule, the proposed regulation should be revised to ensure that there are similar standards and equal oversight and accountability for both IRBs and privacy boards.

L. Enforcement

We recognize that the Secretary is limited in addressing enforcement mechanisms by the delegation of authority in HIPAA. Thus, it is critical that the Congress act to grant people a private right of action to enforce their rights under this regulation.

M. Preemption

We strongly support the approach in HIPAA and the proposed regulations that the federal privacy regulations will act as a floor, but not a ceiling, on privacy protections afforded by the States. Under this approach, weaker State health privacy laws are preempted (or overridden) while State laws that offer more protection than the federal regulations will remain. Furthermore, this approach allows a State, in the future, to enact stronger privacy protections to meet the changing needs of its citizens.

We believe that the regulations should provide definitions of the terminology used in the preemption provisions for general purposes, not just for use in the Secretary's advisory opinions. We also believe that the regulation should treat state laws pertaining to disclosures about minors the same as other state laws generally, preempting state laws that are contrary to the proposed rule and less protective of the privacy of minors. Lastly, we are very concerned about the breadth of the provision under which a State may request a waiver that would allow a weaker State health privacy law to stand, essentially making the analogous federal regulation inapplicable in that State.

V. CONCLUSION

On balance, we believe that the proposed health privacy regulations are a significant and vitally important step towards guaranteeing the American public a greater degree of privacy protection for their medical records. When finalized, the regulation will be the first comprehensive federal rules on health privacy, establishing a minimum set of standards by which health care providers, health plans, and others, must comply. As such, the regulations will not only foster greater public trust and confidence in our nation's health care system, but they will also bring much-needed uniformity and predictability to the privacy rules that must be adhered to across the country. Most importantly, the regulation will establish greater uniformity while leaving states the flexibility to act on behalf of their residents and augment the regulation as needed.

We do believe that it is crucial for Congress to act to fill the gaps in the proposed rule: the regulation should be extended to cover all medical information, whether paper or electronic form; the regulation should cover all of those who generate, maintain or receive protected health information; and the regulation should include a private right of action.

[An attachment is being retained in the Committee files.]

Chairman THOMAS. Thank you very much, Ms. Goldman. Ms. Grealy?

STATEMENT OF MARY R. GREALY, PRESIDENT, HEALTHCARE LEADERSHIP COUNCIL

Ms. GREALY. Mr. Chairman and members of the subcommittee, thank you for this opportunity to testify regarding the proposed HHS regulations regarding the confidentiality of patient information. I am Mary Grealy, President of the Healthcare Leadership Council.

The HLC is an organization of chief executives of the Nation's most respected health care companies and institutions. The views I express today are those of innovative leaders from the full spectrum of American health care, health plans, physicians, hospitals, universities, pharmaceutical, biotechnology, and medical device manufacturers. Our members formed the Healthcare Leadership Council to promote their vision of a consumer centered health system that offers accessible, affordable health care of the highest quality.

The HLC has led a broad-based coalition of 90 organizations and has sought to apply this vision to the issue of patient confidentiality. Our goal has been, and continues to be, legislation that establishes strong, uniform, Federal standards to protect the confidentiality of patient information.

We share the desires of the administration and many members of Congress in this regard. Our members know firsthand how important it is that patients have trust that their medical information will be kept confidential and disclosed only when appropriate.

We appreciate and applaud you, Mr. Chairman, and Congressman Cardin for your efforts to move us closer to the very necessary uniform Federal standards for privacy.

In the absence of legislation, however, we concentrate on the matter at hand, the regulations proposed by Health and Human Services. We share the goal of members of this committee and of the regulations that they must achieve a critical balance. We must give patients confidence that their medical information will be kept confidential and that those who violate the patient's privacy will be subjected to strong penalties.

At the same time, we must ensure that no regulatory barriers will be erected to obstruct the flow of information that has led to virtually every health care advance that has saved and enhanced lives. Can we achieve confidentiality protection without establishing costly regulatory burdens that will divert important resources away from patient care? Striking that balance is the standard that these regulations must meet.

We have determined that in certain critical aspects they fall short of reaching that balance. While there are a number of very positive aspects to these regulations that we can endorse, there are also some ambiguities, gaps and, in some instances, explicit language that will make compliance difficult if not impossible and will have a detrimental effect on the quality and safety of patient care.

Let me make clear at the outset that we support the Department's approach of permitting patient information to be used for payment, treatment, and health care operations without requiring individual authorizations. When individual hospitals and other providers experience millions of patient encounters every day, seeking individual authorizations to disclose information for each of those

encounters would have a catastrophic effect on our health care system and patient care delivery.

Under tab one of my testimony is a chart that illustrates the many integrated components of our complex health care delivery system. Requiring those separate authorizations would impede the flow of information that is needed for the various activities, such as lab tests, ordering prescriptions, immunization programs, and a variety of other encounters, as well.

HHS has handled this important issue properly, and we endorse the approach that they have taken. Now let me address some of the aspects of the regulation that we cannot, at this time, support. My full written testimony addresses this in much more detail, but let me focus on just five areas this morning.

Number one, these regulations become unworkable by attempting to restrict all uses of information as opposed to the disclosure of information. We agree that the limits on disclosure are necessary and appropriate, but attempting to regulate all uses creates a myriad of problems.

Let me put this into prospective. It is inconceivable that regulators in Washington today can predict and define today what necessary use of patient information will be six months from now, much less six years from now. An attempt to do so will really have a chilling effect on the efforts to develop beneficial new uses of patient information.

Number two, these regulations raise questions as to whether population data can be used without unreasonable restrictions to support patient treatment and important health care activities. For example, many health plans today review their entire enrollee database and analyze patterns of emergency room visits and pharmaceutical usage to identify those patients who can benefit from asthma management programs. These are the kinds of things that perhaps, if this regulation is not implemented appropriately or is not clear enough, would be prevented and necessary treatment would not be given.

Number three, there is a two word phrase in these regulations that can have a major detrimental impact on patient care. That phrase is minimally necessary. These rules stipulate that the covered entity must individually review every legitimate request for patient information and provide only that information that is minimally necessary. We have heard that discussed today in the question and answer period, but I think you can detect that this would be a very burdensome requirement given the many patient encounters that occur in our health care system.

Really a catch-22 exists here where you perhaps would have physicians that might be reviewing that request or nurses that are doing the review of those patient records. They would be experts, but that would be a real diversion away from patient care in using those resources. If we decide not to use a physician or a nurse, and we have others do it, there is a real chance that critical information would not be transmitted if they are trying to apply that minimally necessary rule.

Number four, it is also troublesome that the regulations are requiring the cumbersome use of individual authorization for research unrelated to treatment. It is not clear what that phrase un-

related to treatment means. Again, you have heard earlier today some of the concerns raised about the use of that information and the need for having it for medical research that is critical to our health care delivery system.

Finally, Mr. Chairman, it is clear in reviewing these regulations, that HHS has tremendously underestimated the cost. I think Blue Cross Blue Shield has highlighted that very well in their testimony and the study that they had done. The cost burden could have a very serious effect on the cost of health care and the delivery cost, and also on the access to health insurance coverage, about which we are all very concerned.

In this vein, it needs to be emphasized that the Secretary really has, we believe, reached beyond her authority by requiring covered entities to apply these regulations in contracts with their business partners, and to monitor their business partners' activities. We also believe that it is outside the Secretary's authority to impose an implied private right of action, as we think has been done in these regulations.

It is imperative, we believe, that there be a national uniform standard that will provide certainty and clarity to all who are involved in the health care delivery system, patients, providers, researchers and plans.

We look forward to working with members of this committee and Congress, and also working with HHS as they produce this regulation, to see if we can come up with some constructive recommendations. And we think we have done that in the comments that we have submitted. We look forward to working with you and with the Department on this very important issue. Thank you.

[The prepared statement follows:]

Statement of Mary R. Grealy, President, Healthcare Leadership Council

Mr. Chairman and members of the Subcommittee, thank you for this opportunity to testify regarding the proposed HHS regulations governing the confidentiality of patient information.

The Healthcare Leadership Council is the organization of chief executives of the nation's most respected health care companies and institutions. The views I express today are those of the innovative leaders from the full spectrum of American health care—health plans, physicians, hospitals, universities, pharmaceutical, biotechnology and medical device manufacturers. Our members formed the HLC to promote their shared vision of a consumer centered system that offers accessible, affordable health care of the highest quality.

The HLC has led a broad-based coalition of 90 organizations that has sought to apply this vision to the issue of patient confidentiality. My testimony this morning is on behalf of HLC. Our goal has been, and continues to be, legislation that establishes strong uniform federal standards to protect the confidentiality of patient information. We share the desires of the Administration and many members of Congress in this regard. Our members know first hand how important it is that patients have trust that their medical information will be kept confidential and disclosed only where appropriate.

We appreciate and applaud you, Mr. Chairman, and Congressman Cardin for your joint efforts to move us closer to those very necessary uniform standards.

In the absence of legislation, however, we concentrate on the matter at hand, and apply our consumer-centered health care principles to the regulations proposed by HHS. We share the goal of members of this Committee that these regulations must achieve a critical balance. Are we giving patients confidence that their medical information will be kept confidential, and that those who violate a patient's privacy will be subjected to strong penalties? And, at the same time, are we ensuring that no regulatory barriers will be erected to obstruct the flow of information that has led to virtually every health care advance and breakthrough? Can we achieve con-

fidentiality protections without establishing costly regulatory burdens that will divert important resources away from patient care?

Striking that balance is the standard these regulations must meet, Mr. Chairman, and we have determined that, in certain critical aspects, they fall short. There are a number of positive aspects to these regulations that we can endorse. There are, however, ambiguities, gaps and, in some cases, explicit language that will make compliance difficult, if not impossible, and will have a detrimental effect on the quality and safety of patient care.

Let me make it clear at the outset that we support the Department's approach of permitting patient information to be used for payment, treatment and health care operations without requiring the use of individual authorizations. When individual hospitals and providers experience millions of patient encounters every day, seeking an individual authorization to disclose information for each of those encounters -and the transactions resulting from them—would have a catastrophic effect on our health care system and on patient care.

Tab one of my testimony is a chart that illustrates the many integrated component parts of our health care system. Requiring separate authorizations would impede the flow of information needed for various activities such as lab tests, ordering prescriptions, immunization programs, medical research and case and disease management, just to name a few.

HHS has handled this important issue properly, and we endorse their proposed policy in this regard.

Let me address, though, the aspects of these regulations that we cannot, in the name of quality health care, support. My full written testimony addresses our comments in greater detail, but allow me to highlight this morning five areas of particular concern.

Number one, these regulations become unworkable when they attempt to restrict all uses of patient information, as opposed to disclosure of information. We agree that limits on disclosure are necessary and appropriate. Attempting to regulate all uses, however, particularly uses within an entity, creates a myriad of problems.

For example, the regulations create a finite list of narrowly-defined activities for which data can be used without individual authorization.

Let's put this into perspective. In the field of health care, there have been more new strides, developments and breakthroughs, more new ideas, practices and approaches in the last five years than in the previous 25 years combined. It is inconceivable that regulators in Washington can predict and define today what a necessary use of patient information will be six months from now, let alone six years. And to attempt to do so could have a chilling effect on our efforts to develop beneficial new uses of patient data.

Number two, these regulations raise questions as to whether population data can be used, without unreasonable restriction, to support patient treatment and important health care activities. For example, many health plans today will review their entire enrollee database and analyze patterns of emergency room visits and pharmaceutical usage to identify those patients who can benefit from an asthma management program. These regulations are ambiguous, at best, as to whether this would continue to be an acceptable use of patient information without first obtaining an individual's authorization. If it is not, too many Americans will continue to suffer needlessly from treatable chronic conditions.

Number three, there is a two-word phrase in these regulations that can have a major detrimental impact on patient care. That phrase is "minimally necessary." These rules stipulate that the covered entity must individually review every legitimate request for patient information and provide only that information that is minimally necessary.

Beyond the burdensome nature of this requirement -and imagine, for just one hospital handling hundreds of thousands of information transactions a year, how costly and time-consuming it will be—it creates a problematic catch–22. If those reviewing the information are not medical professionals, you run the real risk of excising information that can be critically important to a physician or a medical researchers. If, on the other hand, you assign trained nurses and physicians to review data to determine what is minimally necessary, you are taking vital resources away from patient care. In either case, information critical to treatment and research could be withheld. That could expose patients to harm.

The minimally necessary standard, as proposed, simply will not work.

Number four, it is also troublesome that the regulations require the cumbersome task of individual authorizations for research unrelated to treatment. What does that phrase mean—research unrelated to treatment?" The regulations are not clear, and that ambiguity could lead to restrictions down the line that undermine vital medical research. What we do know is that the great research facilities of this coun-

try—the Mayo Clinic, Johns Hopkins and so many others—do extensive medical research that is not targeted to a particular disease or condition but that results in unforseen and unanticipated health breakthroughs. No regulation should inhibit or undermine this type of research. I have detailed other concerns with the rule's research provisions in my written testimony.

And, finally, Mr. Chairman, it is clear in reviewing these regulations that HHS has tremendously underestimated the impact of these rules on health care costs. The total estimated compliance cost of $3.8 billion over five years fails to account for several new requirements found in these pages. The cost of personnel to determine the minimally necessary amount of information to be disclosed. Requiring health care providers to monitor the practices of their business partners. Establishing and operating federally-mandated privacy boards. The list goes on and on, Mr. Chairman, and the bill to patients, providers and the employers who provide health coverage will be a high one.

In this vein, it needs to be emphasized that the Secretary has reached beyond her authority by requiring covered entities to apply these regulations in contracts with their "business partners" and to monitor those business partners' activities. And, it is outside the Secretary's authority to provide an implied private right of action not envisioned by HIPAA.

Ultimately, as I mentioned earlier, we hope that Congress will pass comprehensive confidentiality legislation. As well intentioned as these regulations are, the Department cannot, under the HIPAA law, preempt state laws that are contrary to or stricter than the federal rules. Thus, as illustrated in Tab two of my testimony, we will continue to have a situation in which the simple act of filling a prescription can involve the separate and sometimes contradictory confidentiality laws of half a dozen or more states.

A nationally uniform standard would provide certainty and clarity for all involved in the health care delivery system—patients, providers, researchers and plans.

We wish to continue to work with you, Mr. Chairman, and the members of this committee to advocate a legislative approach that will protect confidentiality while, at the same time, allow the free flow of information that saves lives and ensures quality health care for the American people.

We will also continue to work with HHS on its regulation and have submitted what we hope are constructive comments to improve this rule.

Again, thank you for this opportunity to testify today.

Summary of HLC Comments on the Proposed HHS Regulations

Since enactment of HIPAA, which set in motion this debate, the HLC has supported several general principles: (1) Patient information should be protected, safeguards should be provided, and patients should have access to their own records; (2) clear boundaries should be set around disclosure of patient information; (3) penalties for violating these requirements should be imposed; (4) patient information should be available for research; and, (5) a nationally uniform set of standards should replace the "crazy quilt" of conflicting, confusing, and sometimes harmful, state laws.

The HLC has thoroughly reviewed the proposed HHS regulations and has submitted extensive comments from a broad industry-wide perspective on aspects of the rule we support, and others that we cannot support without substantial modifications. The following will highlight our comments on the proposed rule.

Aspects Of The Proposed Rule HLC Supports

Allowing Disclosure/Use Without Authorization For Appropriate Activities

The HLC supports the Department's approach of permitting patient information to be used for payment, treatment, and healthcare operations without requiring entities to obtain individual authorizations. This so-called "statutory authorization" approach is clearly correct. Alternative approaches requiring separate authorizations from the individual each time information is disclosed or used for appropriate health care activities would seriously disrupt our health care system and harm patient care.

For example, providers routinely order tests and other services through unrelated providers (such as laboratories or radiology services), not all of which have contact with a patient. Family members routinely pick up prescriptions for a sick family member at home. Each of these potential exchanges of information could be subject to separate authorizations by the individual under multiple authorization schemes.

Health plans often cover spouses, dependents, and even children not living with the parent who subscribes to the plan. Collecting authorizations from these individuals could create serious obstacles for the delivery of health care services.

The potential harm caused by such multiple authorization schemes is not idle speculation. Maine passed such a law that was so disruptive it was repealed in an "emergency" bill just 14 days after taking effect.

Some Americans still view our health care delivery system as the relationship between patient, doctor, hospital, and pharmacist. The reality, of course, is that our system has evolved into a highly integrated, complex, and, as a result, better delivery system. Tab one of HLC's testimony illustrates the many integrated component parts of our health care system. Requiring separate authorizations to allow information to move among these components would be highly disruptive and compromise patient care.

We do have concerns with several limitations put on the "statutory authorization" which are discussed later.

Including Important Health Management Activities

The HLC also supports the inclusion of treatment, payment and health care operations in the activities for which no individual authorization is needed. We are pleased that the Department recognized the importance of such activities as case and disease management to patients by including them in their definitions. Disease management programs for chronic diseases such as asthma, diabetes, heart disease, and others are dramatically improving the lives of millions of Americans. We do have concerns with some limitations on these programs which we discuss later.

Other Allowed Uses and Disclosures

The HLC supports the need for disclosure to public health authorities and is pleased that the rule allows disclosure to someone complying with such an authority. We also support the need for the disclosure to health oversight agencies to improve

health care quality and protecting public health, as well as for government health data systems.

Research

Finally, the HLC supports the general direction of the research provisions of the rule to the extent it does not require individual authorization for disclosure of data to research entities. We do have some major concerns about the research provisions will be discussed later in our testimony.

Provisions of the Proposed Rule of Concern to HLC

Regulating Use of Information

While the HLC supports the need for the rule to restrict disclosure of patient information outside of appropriate entities, we are concerned about the numerous and burdensome restrictions on the uses of such information, particularly uses within a covered entity. These restrictions on use of information create several problems.

- The rule prohibits all internal uses of data that do not fall in to a relatively narrowly defined set of activities. The Department is, thereby, taking the position that it can define all conceivable appropriate uses of patient information. We believe that this is not only impossible for current uses, but such an approach would have a chilling effect on the development of beneficial new uses of patient information.
- The HLC is concerned that the rule will unduly limit the use of population data that is used to support patient treatment and other legitimate activities. This is because the allowable uses of patient information are closely tied to the provision of health care to an individual patient. This raises a question as to whether, for example, a health plan could review an entire enrollee database to identify specific individuals whose utilization patterns of asthma drugs, or emergency room visits, indicate they would benefit from being enrolled in an asthma management program.
- Again, because an entity's internal uses of patient information are so sharply restricted by the rule, several important internal business operations of health care providers and plans could be left out. For example, a national health plan recently undertook a study to evaluate the cost effectiveness of its preauthorization requirements. Audits of real cases containing patient information were necessary. The audit resulted in the plan dropping some preauthorization requirements, a good result for patients and the plan.
- The HLC is concerned that the definitions of treatment, payment, and health care operations may be diluted by the rule's approach broadly defined as "marketing." If a use or disclosure is deemed to be for the purpose of marketing—a term

not defined—an individual authorization would be required. This determination could be made on a retrospective basis and could be applied to certain types of disease management programs, and also the use of formularies by health plans, and providers (most notably hospitals). For instance, a candidate for an asthma disease management program may receive a more effective drug therapy under a disease management program. There is the risk that under the rules such activities could be viewed as marketing activity. To the extent arrangements fall within the definition of treatment, payment, or health care operations, they should not be subject to conflicting rules under "marketing."

The HLC recommends that the rule focus on restricting disclosure of patient information, not use (particularly use within an entity). At a minimum, internal management functions of providers and plans that involve only the use, not disclosure, of patient information should be broadly included under the definition of health care operations.

Minimum Necessary Rule

The rule requires that entities "review each request for disclosure individually on its own merits [from preamble]" and determine which information is minimally necessary. It is neither practical nor consistent with good medical practice to promote a rule that would encourage and possibly require excision of data in a medical record. The recent Institute of Medicine report underscores the potential harm to patients when providers have only limited access to information. The HLC suggests that, alternatively, entities be allowed to have general practices and guidelines and not be required to make individual determinations.

Unnecessary Administrative Burdens

- The HLC is concerned that the requirements for accounting for the disclosure of patient information, detailed provisions governing the practices of "business partners" and their relationship with covered entities, and the training and certification requirements will greatly increase the administrative burden borne by covered entities.
- The Department has exceeded the scope of its authority under HIPAA in several provisions, most notably in those provisions pertaining to the "business partner" of a covered entity. And, it is outside the Secretary's authority, and not envisioned by HIPAA, to provide an implied private right of action.

De-identifying Data

The HLC has serious concerns that the standard for de-identifying data in the rule sets the bar too high. Requiring that 19 identifiers—including even "account numbers" and "zip codes"—be removed to de-identify data would make data anonymized and nearly worthless to most researchers. The practical effect of this standard will be to discourage, rather than encourage, encryption and other efforts to de-identify records. The HLC recommends that these "identifiers" be limited to a more reasonable list of characteristics that truly identify individuals.

Research

- The HLC believes that modifications to the Institutional Review Board (IRB) process should be addressed separately in a comprehensive review of the IRB process and not via this rule. Several of the criteria to be used by an IRB (or "privacy board") exceed the Department's authority by regulating the content of research, as opposed to overseeing the confidentiality of data in research.
- The requirement that individual authorization be obtained to use data in "research unrelated to treatment" is unworkable and unnecessary.
- The HLC is concerned that the disclosure or use of data may be subject to the "minimum necessary" requirements mentioned earlier.

National Uniformity

One of the primary reasons HLC supports comprehensive legislation to protect confidentiality is the need to provide a nationally uniform standard. The confusing and contradictory patchwork of state laws is an ineffective -and sometimes harmful—approach to regulating a highly integrated and decidedly interstate health care delivery system.

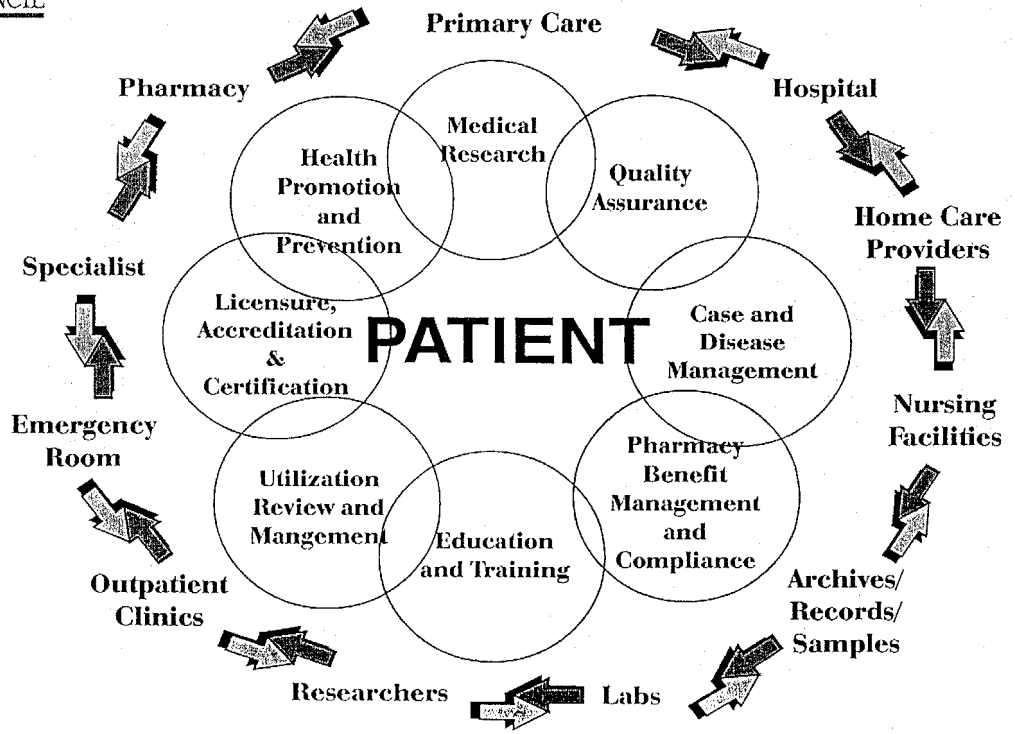
An illustration of why state confidentiality laws are inappropriate in health care is included under tab two of my testimony. In this example, a college student living in New York is prescribed a medication in New Jersey. Before the transaction is completed, entities in seven states are involved. Which state's confidentiality laws apply? The answer is "all of them!"

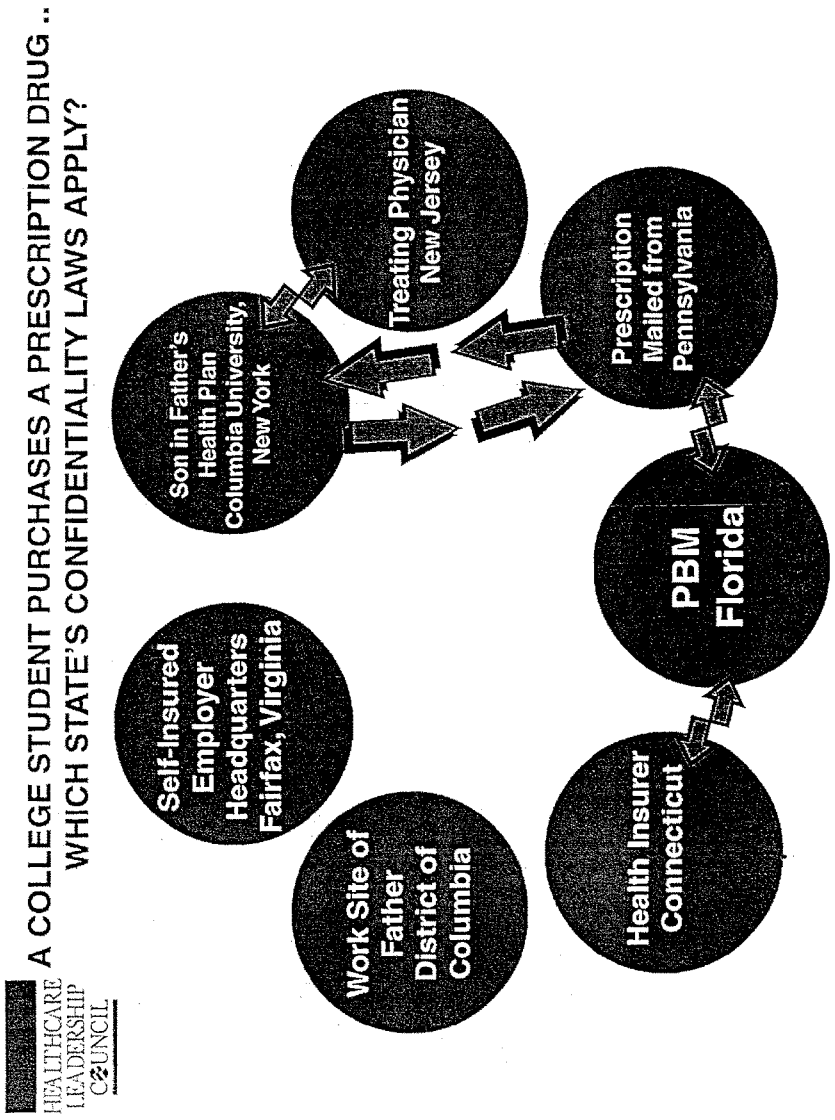
The HLC has examined all of the state confidentiality laws on the books, and many more being proposed, and concludes that a nationally uniform standard would do more to protect the confidentiality of patients' information than any other single reform. Such a nationally uniform standard would provide certainty and clarity that would at once protect patients and not unduly burden health providers, plans, and others.

Of course, under HIPAA, the Department does not have authority to preempt state laws that are contrary or stricter than the federal rules. Thus, the need for comprehensive legislation. At the very least then, the HLC believes that it is incumbent upon the Department to evaluate state laws and provide guidance to covered entities regarding which state standards covered entities should follow.

HEALTHCARE LEADERSHIP COUNCIL

THE VALUE OF PATIENT INFORMATION FOR QUALITY CARE IN AN INTEGRATED DELIVERY SYSTEM





Chairman THOMAS. Thank you very much, Ms. Grealy. Dr. Ober?

STATEMENT OF N. STEPHEN OBER, M.D., PRESIDENT AND CHIEF EXECUTIVE OFFICER, SYNERGY HEALTH CARE, WALTHAM, MASSACHUSETTS

Dr. OBER. Chairman Thomas, members of the subcommittee, thank you for the opportunity to appear before you today. My name is Stephen Ober. I am a physician and President and CEO of Synergy Health Care, a health research and data analytics company headquartered in Waltham, Massachusetts.

Synergy is a subsidiary of Quintiles Transnational Corporation, the largest contract research organization in the world and a leader in health care informatics services. As a subsidiary of Quintile, Synergy is an affiliate of ENVOY, the largest claims clearinghouse in the United States, which processes an average of 3.5 million electronic data transactions per day, providing connectivity between 270,000 providers and 800 payers. I have been part of a Quintiles work group which has closely analyzed the NPRM in relation to its impact on claims clearinghouses and their business partners.

Let me begin my comments by stating that Synergy and Quintiles, in general, believe that the proposed NPRM standard to protect the privacy of individually identifiable health information are reasonable. However, I would like to offer four brief comments.

First, clearinghouses are defined as covered entities by the rule. But because clearinghouses are also business partners of providers and health plans and do not have direct relationships with patients, several requirements of the rule appropriately do not apply to clearinghouses, such as providing a notice of information practices, and offering access for inspection or copying of records. We applaud this sensible approach and fully support the concept that clearinghouses and other business partners would not be permitted to use or disclose identifiable health data in ways not permitted to the covered entity to which such information was initially provided.

We are concerned, however, by the provision that would require a covered entity, when acting as a business partner of another covered entity—as claims clearinghouses always do—to be bound by the health information policies and procedures of its partners. Thus, the health care clearinghouse would have to establish its own privacy policies and procedures, but then be required to attempt to adhere to the privacy policies and procedures of the thousands—and I do mean thousands—of other covered entities for which it acts as a business partner.

This approach would needlessly complicate the network of existing relationships and be practically impossible to administer.

Second, the NPRM stipulates that covered entities must have each business partner sign a contract which details the uses of identifiable health information and requires its protection. Again, we agree with this principle. However, we suggest that HHS should adhere to its stated intention of promoting de-identification of individual health information whenever possible by clarifying that business partners who are in lawful possession of identifiable health information may create de-identified health data and, in fact, should be encouraged to do so.

Third, in the NPRM, the Department proposes to establish a safe harbor for the creation of de-identified health information if cov-

ered entities eliminate 19 potential individual identifiers. While we agree with the elimination of most of the identifiers mentioned, eliminating others would negatively impact the ability to use these data in research activity.

For example, certain geographic identifiers and patient date of birth are two of the most important demographic data elements required in performing most health care research. The rule, as written today, requires elimination or modification of these valuable elements.

Finally, one of the most exciting potential of health care clearinghouses, and the one I am personally most passionate about, lies in the capacity to create de-identified data on a large scale.

In the NPRM, HHS comments on the "many instances in which such individually identifiable health information is stripped of the information that could identify individual subjects and is used for analytical, statistical, and other related purposes." This is, in fact, what we do at Synergy.

For instance, one study for the Centers for Disease Control, we showed that the use of hepatitis B vaccine by physicians decreased dramatically following several reports of adverse effects of this immunization, something CDC had been struggling to monitor for several months. In another, we were able to illustrate the positive impact of an education program aimed at increasing appropriate physician testing and treatment of the bacteria that causes peptic ulcer disease, a curable illness today. In working with a major drug manufacturer and the FDA, Synergy's timely monitoring of a patient prescription usage patterns lead to a withdrawal of a previously used drug.

And yes, Mr. Chairman, we have also done work looking at medical errors. These are just a few examples of what are virtually limitless uses of de-identified health care information.

While we are most supportive of the NPRM rule as a covered entity and a business partner, we at Synergy and Quintiles want to be certain that all parties realize the impact of these regulations, if not carefully derived, could have on the status of health care research.

On behalf of Synergy Health Care and Quintiles Transnational, thank you for the opportunity to appear before you today.

[The prepared statement follows:]

Statement of N. Stephen Ober, M.D., President and Chief Executive Officer, Synergy Health Care, Waltham, Massachusetts

Chairman Thomas, Members of the Subcommittee: Thank you for the opportunity to appear before you today to discuss provisions of the proposed regulation relating to the operations of health care clearinghouses, the creation and use of de-identified health information, and the preemption of state laws.

My name is Stephen Ober. I am a physician and President and CEO of Synergy Health Care, a health research and data analytics company headquartered in Waltham, Massachusetts. Synergy is a subsidiary of Quintiles Transnational Corporation, the largest contract research organization (CRO) in the world and a leader in healthcare informatics services. As a subsidiary of Quintiles, Synergy is an affiliate of ENVOY, the largest claims clearinghouse in the United States, which processes an average of 3.5 million electronic data transactions per day, providing connectivity between 270,000 providers and 800 payers. Some of you may have read of the pending purchase of ENVOY from Quintiles by Healtheon/WebMD. As part of this transaction, Synergy will continue to receive de-identified data from ENVOY, maintaining our historic ties. The matters before this Subcommittee regarding data privacy

and medical research have been of constant interest to our family of companies. I have been part of a Quintiles workgroup, which has closely analyzed these matters, including the NPRM and its relation to the impact on claims clearinghouses and their business partners, and I am happy to speak to you on this topic today.

Health Care Clearinghouses

As you know, one of the objectives of the Health Insurance Portability and Accountability Act (HIPAA) was to improve the efficiency and effectiveness of the health care system, "by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." One reason why HIPAA was so crucial is demonstrated by the rapid growth in the electronic transfer of health information: today 62% of all healthcare claims are processed electronically, and for hospital and pharmacy claims the percentage is over 80%. In 1998 some 2.7 billion out of a total of 4.4 billion claims were processed electronically, an important factor in ongoing efforts to improve the efficiency of our health care system and reduce health care costs.

In a section on "administrative simplification," HIPAA directed HHS to adopt a series of standards that would encourage uniformity for a range of electronic health information transactions. The proposed standards for the privacy of individually identifiable health information that is maintained or transmitted electronically were also mandated by HIPAA in the absence of the passage of comprehensive medical records privacy legislation by Congress. The NPRM proposes standards to protect the privacy of individually identifiable health information, outlines the rights of individuals who are the subject of this information, and defines the authorized and permitted uses of identifiable health information. In general, Synergy and Quintiles believe that the proposed rule establishes reasonable standards for security and efficiency of the health information infrastructure. We applaud HHS's efforts to encourage the de-identification of health care data for medical research.

The "covered entities" defined by HIPAA include health plans, health care providers that transmit health data electronically, and health care clearinghouses. Although clearinghouses are indeed covered entities, the proposed rule recognizes that they are also "business partners" of the health care providers or health plans for whom they are processing the full range of administrative transactions and providing connectivity. Because claims clearinghouses do not have any relationship with individual patients, the NPRM appropriately does not apply several requirements that must be followed by health plans and providers. These include, providing a notice of information practices, offering access for inspection or copying of records, and accommodating requests for amendment or correction.

We endorse this sensible approach, and support the concept that clearinghouses and other business partners would not be permitted to use or disclose *identifiable* health data in ways not permitted to the covered entity to which such information was initially provided. We are concerned, however, by the provision that would require a covered entity, when acting as a business partner of another covered entity (as claims clearinghouses always do), to be bound by the health information policies and procedures of its partners. Thus, a health care clearinghouse would have to establish its own privacy policies and procedures, which is entirely sensible, but then be required to attempt to adhere to the privacy policies and procedures of the thousands of other covered entities for which it acts as a business partner. Obviously, this approach would needlessly complicate the network of existing relationships by which health care is delivered and paid for today, and potentially thwarts the administrative "simplification" HIPAA meant to foster. In our written comment, we have requested that HHS clarify this provision, as it appears redundant and more likely to produce confusion than improved protection of identifiable health information.

Creation and Use of De-Identified Health Information

The NPRM stipulates that covered entities must have each business partner sign a contract which details the uses of identifiable health information and requires its protection. Again, we agree with the principles that the use of identifiable health information by a business partner can be limited by contract and that business partners are not permitted uses or disclosures not allowed to the covered entity. However, we suggest that HHS should adhere to its stated intention to encourage de-identification of individual health information whenever possible by clarifying that business partners who are in lawful possession of identifiable health information *may create* de-identified health data and, in fact, are encouraged to do so.

In the preamble to the proposed rule, HHS suggests that covered entities *and* business partners would be encouraged to create de-identified health data and

"would be permitted to further use and disclose such de-identified information in any way, provided that they do not disclose the key or other mechanism that would enable the information to be re-identified, and provided that they reasonably believe that such use or disclosure of de-identified information will not result in the use or disclosure of protected health information."

One of the most exciting potentials of health care clearinghouses lies in the capacity to create de-identified data on a large scale. Certainly, using de-identified data for health research affords the greatest security for patient privacy, and the Department hopes that de-identified data would always be used when it is sufficient for a given research purpose. In the NPRM, HHS comments on the "many instances in which such individually identifiable health information is stripped of the information that could identify individual subjects and is used for analytical, statistical and other related purposes" such as epidemiological studies, comparisons of cost, quality or specific outcomes across providers or payers, studies of incidence or prevalence of disease across populations, areas or time, and studies of access to care or differing use patterns across populations, areas or time." In regard to the activities of claims clearinghouses, the NPRM suggests that such covered entities "could want to use codes or identifiers to permit data attributable to the same person to be accumulated over time or across different sources of data" and, further, that a "business partner generally could create a database of de-identified health information drawn from the protected health information of more than one covered entity with which it does business, and could use and disclose information and analyses from the database as they see fit, as long as there was no attempt to re-identify the data to create protected health information."

At Synergy we use de-identified, aggregated health information to provide real-time data analysis to improve pharmaceutical and medical service outcomes. For instance, in one study for the Centers for Disease Control (CDC), we showed that use of the Hepatitis B vaccine by physicians decreased following several reports of adverse effects of this immunization—something CDC had been struggling to monitor. In another, we were able to illustrate the positive impact of an education program aimed at increasing appropriate physician testing and treatment of the bacteria that causes peptic ulcer disease. In working with a major drug manufacturer and the FDA, Synergy's timely monitoring of patient prescription usage patterns led to the withdrawal of a previously approved drug. These are only three examples of what are virtually limitless uses of de-identified health information.

In the NPRM, the Department proposes to establish a "safe harbor" for the creation of de-identified health information by stipulating that "[a] covered entity may use protected health information to create de-identified information by removing, coding, encrypting, or otherwise eliminating or concealing" nineteen potential identifiers. Thus, regardless of a large or small population size, anyone removing all of these nineteen identifiers to create de-identified information could safely conclude that the information is not identifiable. As we have posed in our comments to the NPRM, the problem is that the anonymized data produced by this "safe harbor" method and the resulting aggregated database has little value for research purposes.

For example, the list of nineteen identifiers includes information such as "city, county, zip code, and equivalent geocodes." However, in order for de-identified data to be useful as health research, researchers must have a means to track information demographically. By excluding all means of demographic analysis, i.e., city, county, zip code and equivalent geocodes, the value of such health research would be diminished greatly. In our written comment we recommend that to maintain demographic value of the de-identified data, some geographic locators should be excluded from the list of nineteen identifiers. We are aware that there is a higher probability of identifying an individual if a nine-digit zip code is included as an identifier. By retaining city, county and five-digit zip code in the de-identified data, however, the probability of identifying an individual would be reasonably low.

Similarly, HHS includes "[b]irth date" in the list of identifiers that must be removed or concealed to qualify for the de-identification safe harbor, but would allow age to be retained. However, the actual date of birth is of critical value for research purposes. For example, without date of birth it would be impossible to perform research on neonatal and pediatric populations. In these age groups differences in health status are measured in weeks and months, not years. Access to date of birth also avoids any of the ambiguities in assigning patients to age cohorts that can mire research efforts and produce erroneous results. For example, it may be unclear when a patient labeled as "35 years old" was actually that age—was it when they joined their health plan, saw their physician, or submitted their medical claim. Accordingly, retaining the date of birth or, at least, month and year of birth would be critical to research and produce higher quality results.

In the NPRM, HHS proposes an alternative method for the creation of de-identified data, that is, "entities with appropriate statistical experience and expertise may treat information as de-identified" even if it contains one or more of the nineteen "identifiers." We appreciate that HHS has provided concrete guidance regarding de-identification for entities that need it, but allows a sophisticated entity, using a standard of "reasonableness," to make a determination whether sufficient information has been removed so that "the result is still a low probability of identification." Nevertheless, even sophisticated users could decide to utilize a reasonable "safe harbor" that established a presumption of de-identification. Such a universal safe harbor would allow a framework that would serve as a benchmark for all, promoting uniformity in the health care industry and providing greater comfort to individuals with respect to their privacy.

While I have focused on the potential impact of the proposed rule on health care clearinghouses, and the creation and use of de-identified data, I must comment briefly on the preemption of state laws. The proposed rule would establish a floor and preempt only those state laws that provide "less stringent" privacy protection. However, allowing states to create more stringent standards governing particular kinds of information or certain entities will create a confusing and ineffectual array of requirements. The proposed rule provides a logical and reasonable federal standard for "authorized" uses, but without preemption of state laws there can be no uniformity of protections or consistent guidance concerning the handling of identifiable health information for health plans, providers, researchers or, most importantly, patients.

On behalf of Synergy Health Care and Quintiles Transnational, thank you for the opportunity to appear before you today. I will be happy to answer any questions.

Chairman THOMAS. Thank you very much for your testimony, Doctor, and I do thank all of you for the far more extensive written testimony. My assumption that your submission to HCFA is also far more extensive.

Dr. Plested, your position is one which I think is fairly recognizable in terms of physicians, the desire to protect that relationship between the doctor and the patient. Does the AMA or, if they do not have a position do you as a practicing physician, have any concern about the fact that the access to data, even if we were to restrict it to just the physician and the patient, is a two-way street under this structure? That is, patients have the right to look at data and, in certain instances, "correct" the data?

Does that concern you all about whether or not the integrity of the medical record could be compromised, by the patient's ability to make changes?

Dr. PLESTED. There is no question that in certain instances that is true, Mr. Chairman. I am sure Dr. McDermott can tell you, from the point of view of a psychiatrist, that there are times when it is not in the best interest of a patient that he continually review the chart and the notes that are made about him. We feel that it is important that the patient be a part of the treatment and we have suggested repeatedly that excerpts or that summaries should be prepared for all patients. Whether or not every patient should look at everything that is written, we are afraid, will lead to a practice of omitting sensitive material from records that physicians keep.

Chairman THOMAS. One of the reasons it is really hard to get this done is that it goes to the heart of who we are and how we operate. Whenever you deal with individual rights versus public rights, in trying to get that proper balance, especially in today's information rich world, it is very difficult. Look at the Bill of Rights.

It starts out Congress shall make no law, and then away we go over the centuries, making laws. So it is a very difficult thing.

Doctor, in trying to reconcile this individual versus the public rights relationship, do you believe that it is appropriate for us to collect the data, notwithstanding the very strong statement you have made, to attempt to get at the heart of the accidental deaths, upwards of 100,000, that the Institute of Medicine's To Error is Human Report indicates? That is, use this data for the public good, attempting to collect it in a way to examine practice procedures which might be collected in a systemic way to reduce medical errors?

Is that a public good that you place fairly highly or low?

Dr. PLESTED. Well, there is no question that the AMA is strongly on record that this is an absolute public need and a public good, and that is why we established the National Patient Safety Foundation, who I am sure you are quite familiar with. The question is how much sensitive, personally identified data is necessary for this type of activity to be carried out? I think that is debatable. There would be those who say that they must have access to all.

Clearly that is not the case. We can do this type of a job that must be done and we support being done without having free access to everything in a patient's medical record.

Chairman THOMAS. Of course, if the choice is all or nothing, we would not be here and we would all be home already.

Ms. Fox, you heard the testimony of HCFA, that they felt fairly comfortable about their $3.8 billion cost over five years. You have indicated that it is somewhere near $40 billion.

It is very disconcerting when you get those kinds of ranges. My assumption is that the lower the amount, I would put to you, the stronger you or Ms. Grealy or others would feel about the number being accurate. For example, if I said let us just cut it in half, and you go from $40 billion to $20 billion, and let us take their number and double it from $3.8 billion to $7 billion, that is still a pretty wide range, in terms of what the costs are going to be rippling through the system.

I think that is your concern. Did you submit information which might assist HCFA in looking at the final reg, getting a better understanding of what your concerns were about where the cost centers might be that they had not appropriately looked at?

Ms. FOX. Yes, we did, Mr. Chairman. I think one aspect is in their preamble to their proposed rule, they stated that there were a number of the areas they just did not have data to base the estimate. Three of the 10 areas they mentioned were areas that we thought were particularly expensive that we did very detailed estimates. We have met with them. We have submitted all of our materials, the backup materials. We have also met with the General Accounting Office, the Congressional Budget Office, and others, because we thought it would be really helpful for everybody to really take a look at some of these assumptions.

I will just give you one example of where they did make an estimate where our estimates are very different, just to give you a sense of perspective. The regulation requires everybody to train their employees about these new privacy rules. We estimated, we assumed that employees would spend one to two hours over the

five year period learning about privacy rules. We do not know what their hourly estimates were, but I can tell you for health plan their preamble says an entire health plan would spend $100 training their employees.

I can tell you, as an employee of Blue Cross Blue Shield Association, on virtually any issue we get training on, we spend an entire day and it is a mandatory training. I do not know that we would do that on this, but $100 a health plan is just way underestimating the cost of training your employees.

Chairman THOMAS. Especially if you get caught in the web, it could be $250,000. The $100 would not have been well spent. What usually occurs in those instances is the dollar amount goes up in relation to the potential downside. I agree with you, $100 sounds a little short, especially with what $100 can buy today.

Ms. Goldman, how many pages of information did you submit to HCFA?

Ms. GOLDMAN. We submitted nearly 120 pages of comments.

Chairman THOMAS. And yet your testimony indicated you were pretty supportive of the direction that they were going, yet you found 120 pages worth of areas worthy of commenting on?

Ms. GOLDMAN. Not to be accused of being verbose, we were mindful of the request the Secretary made when she issued the draft, that we should comment both on the things that we thought should be strengthened, and on the provisions we thought should be maintained.

In addition, we had a number of groups sign on to our comments. And so each section of the regulation that we comment on also has the sign on of the supportive groups. So not every piece of paper is taken up with substantive comments, but there are about 120 pages.

Chairman THOMAS. Good, because I know that you were instrumental in producing for the this Health Privacy Project, the Best Principles for Health Privacy. I just have to tell you that I was a little concerned, as this group pulled together, that given the cross-section of individuals involved, which again was a very representative sample, and the ability to—I am sure there were differences—to resolve them and present specific examples for principles. One has been very helpful to me and I know, too, the gentleman from Maryland, in our looking at what we are doing, so I was interested.

You made a comment and I want people to understand it, because you said in the area of law enforcement it fell short. What you meant by saying that it fell short was that there were not enough individual protections, vis-a-vis the ability of Government to get at data for what may or may not be worthwhile reasons. That is what you meant by falling short?

Ms. GOLDMAN. Exactly.

Chairman THOMAS. Because if somebody heard it and said you thought law enforcement fell short they might, if they did not know you, think it was the other way.

Ms. GOLDMAN. We hope, and we have not looked obviously at all of the comments that have been submitted as of today, all of the 40,000, but our hope, based on everything we have heard in the last few years, after the Secretary issued her recommendations, is that every single group, the consumer groups, disability rights

groups, the health plans, providers, researchers, all think that law enforcement should be required to present some kind of legal process that is issued by a neutral magistrate and has a strong standard in it.

I realize internally, within the administration, there is a debate over how that should be handled. We are hoping that they come down on the right side and strengthen that section.

Chairman THOMAS. But on a continuum, would you say that it is fair that, in comparison to the Secretary's first attempt in dealing with the records and law enforcement, that this most recent attempt is an improvement? Have you seen movement, significant movement, modest movement, not enough to really count?

Ms. GOLDMAN. Her initial recommendation said we should maintain the status quo, which is essentially unfettered access by law enforcement to people's medical records. So in a few years they have moved from that to saying here are three options that law enforcement can choose from that the covered entities can acknowledge, three options.

Our concern is there is no guidance in the proposal as to when law enforcement should choose which option. So if information is highly sensitive and there is a serious risk of abuse, they could get an investigative demand that issues internally and that is just as sufficient as getting a warrant or a subpoena.

So in some ways, it appears to be an improvement, but I think that it is a little misleading.

Chairman THOMAS. It may be the appearance, rather than actual.

Ms. GOLDMAN. Exactly.

Chairman THOMAS. Dr. Ober, your background and your business is an interesting one. Your description of it and the terminology you use is more and more becoming commonplace, about these companies that do not make widgets but provide very significant services to the society. There was an old ditty about big bugs have bigger bugs that jump on them and bite them, and bigger bugs have bigger bugs and so on, ad infinitum.

This business of having entities that you articulated very clearly, nevertheless creates this kind of rotational aspect. Did you submit information to HCFA to assist in perhaps breaking that—if it is not a catch-22, it certainly is a big bugs have bigger bugs cycle?

Dr. OBER. Yes, we did our best.

Chairman THOMAS. Given the way you deal with information, are there ways to—

Dr. OBER. Sir, I think in what we submitted we tried to be quite clear in the myriad of business partners that we have and who Synergy is and what Synergy's mission is, as distinct from the claims clearinghouse partners that we have that submit the de-identified data directly to us.

Chairman THOMAS. I am very interested in this business of de-identified data, notwithstanding the identifier, since especially in dealing with electronics you can flag and do a number of things that allows you to deal with de-identification, but if something comes up you can go back and look up a critical or health care nature.

But most importantly, the absolute desperate need for broad-based data for outcomes research and for medical errors correction. We simply would not be able to make significant progress in those two areas. One, cost saving is very important. And the other, life-saving is very important and we appreciate the data that you have and I may want to tap into it.

The gentleman from Washington?

Mr. MCDERMOTT. Thank you, Mr. Chairman.

I would say that, having done this for a few years, I recognize the technique of burying people in paper and giving inflated estimates and doing a lot of things to create confusion, which stops things. I looked at that cost estimate that you put out and I do not want to spend my five minutes going through all of it, except to say that one of the things that was assumed by your contractor, Ms. Fox, was that there would be rules requiring new authorizations from current subscribers to use their data for treatment, payment of claims, or other health care plan options. And they estimated it for you at about $2 billion.

Now the fact is that the proposal does not require providers or health plans to obtain patient authorization to use data for treatment, payment, or health care operations. So they created a burden and put a $2 billion tag on it. That is just one. There are a whole series.

I think that if we are going to make the decisions here on the basis of what privacy is worth, then we ought to be real careful about how we estimate what it is going to cost. Because maybe we say to the American people we do not care about your privacy because it is going to cost too much. If that is the way we make the decision here, we will have a serious problem.

I do not think the Chairman or I, or anybody else, and I think when you get these kind of estimates where clearly there are other things in here that I can go through, you have to be careful about using that because I think you create a problem for yourself.

Dr. Ober, let me ask you a couple of questions, because I have a diagram about how your company operates. I was trying to figure out what kind of health information do you get and from whom do you get it?

Dr. OBER. Currently, our stream of health care information is electronic, de-identified and encrypted data from ENVOY Corporation, which is as I mentioned earlier the country's largest claims clearinghouse. It is, from Synergy's standpoint, a single source, as a go-between between the providers of health care and the payers of health care, ENVOY has set up, over years and years, very standard formats in encryption technology, such that Synergy is the daily recipient of those data streams.

Mr. MCDERMOTT. It is not individually identified?

Dr. OBER. No, sir.

Mr. MCDERMOTT. It is all de-identified?

Dr. OBER. It is de-identified and encrypted; that is correct. At Synergy's end we "use" the pharmacy data and the medical data to do our work.

Mr. MCDERMOTT. But you use that data, it comes over the Internet?

Dr. OBER. No, sir, it comes through a direct T–1 hookup between Nashville and Boston, Massachusetts.

Mr. MCDERMOTT. You have one line that goes all the way?

Dr. OBER. Yes, sir.

Mr. MCDERMOTT. And nobody can break into that?

Dr. OBER. No, sir, it is a dedicated, dial-up line, security.

Mr. MCDERMOTT. As we have watched recently, there have been some privacy breaches in health-related websites. You are saying, in public and on the record, that there is no way anybody can break into your system?

Dr. OBER. I would not be that naive, to say that there is no way someone could, sir. I think there is probably three or four levels, when you think about what we mean by security in the technology age today. And there is a major difference between Internet technology, as we know it in common parlance, and also the dial-up direct networks that we have set up with ENVOY. So that the multiple levels of security that we have, and certainly the fact that it is not Internet right now, and that it is a direct dial-up, which offers one level of security.

Secondly, if someone were to get into our "network" as does happen every now and then, there are no less than three levels of firewall and security checks, passwords and double passwords and changing passwords, that one would need to crack that.

But then we are also offered a third level, which I think is quite valuable to the business we are in. And that is, if somebody were, God forbid, to get into our claims level database, it would almost be nonsensical because it is still encrypted. Certainly, it is already de-identified. But on top of that, most of the data we have in our warehouse, in our database, is alpha-numeric codes that to a layperson would mean nothing, such as an 11-digit for a particular pharmaceutical. They would have to know that digit means a particular drug.

Not infallible but certainly, we think, offers quite a bit of protection.

Mr. MCDERMOTT. When your company sells ENVOY to WebMD, as they are in the process, what are they selling to WebMD?

Dr. OBER. The assets of the transaction business.

Mr. MCDERMOTT. What are you giving them?

Dr. OBER. It is a company of X numbers, hundreds of employees, and the technology that goes into transacting the process of those claims from providers to payers.

Mr. MCDERMOTT. But no access to any database?

Dr. OBER. No, sir.

Mr. MCDERMOTT. You are just selling the people; is that what I understand?

Dr. OBER. Peoples, computers, hard assets.

Mr. MCDERMOTT. Why would WebMD buy that bunch of people and not want the database that they have?

Dr. OBER. You would have to ask Mr. Arnold.

Mr. MCDERMOTT. How did they cut them off?

Dr. OBER. Well, we still are going to—

Mr. MCDERMOTT. Did they say we will leave this over here, you can buy everything but the database?

Dr. OBER. We were very much arms-length from day one with ENVOY because we have set up these very elaborate encryption and de-identification processes.

Mr. MCDERMOTT. It does not look like there is much arms-length when you see this, it says product development and commercialization. You are down in the—

Dr. OBER. Informatics.

Mr. MCDERMOTT. Informatics. You gather the information and pass it to the product development, who then commercialize it. That is what your diagram, that is what your promo is?

Dr. OBER. Yes, and that is maybe confusing. I would have to look at it. But what Synergy's core business is, again, it is medical research and it is analyzing transaction data which we receive encrypted and de-identified from ENVOY. It has always been our business, even prior to joining Quintiles and that organization.

Mr. MCDERMOTT. With your indulgence for just a second, then what are you worried about? This is de-identified?

Dr. OBER. Correct.

Mr. MCDERMOTT. So what are you worried about?

Dr. OBER. Absolutely nothing.

Mr. MCDERMOTT. You came down here to Washington to testify—

Dr. OBER. I was asked to testify, particularly I think based on the value of de-identified health care information for the public good, as we have met with Mr. Cardin and others throughout the last several months. Quintiles is a very large organization, and we have clinical research groups, commercialization groups, and of course informatics.

We wanted to really rest assured that the ability for our business partners to do the de-identifying and continue to pass that very valuable stream to us, to do our business, would not be impeded by the regs. And as near as we can tell, it really is not.

Mr. MCDERMOTT. But what is the problem, when the regulation simply requires the contract between you and the people who are shipping this de-identified information to you, you are a big company. Why would you bristle or object to signing a simple contract and say we are not going to give away information that we do not have anyway? What is the problem with that?

Dr. OBER. I went over the three or four points that we were concerned about in my testimony, and which we have submitted. We wanted to really rest assured that our ability to do the de-identification, receive de-identified data, would not be encumbered by the regs. And the early drafts were still questionable.

I think the rule, as we have read it today, we appear to be very comfortable with it.

Mr. MCDERMOTT. So you are setting up a false ghost here, and you are now clobbering it; right? We do not want that ghost? Because it is not in the regs now.

Dr. OBER. We are certainly glad to hear you say that and we agree that most of what we were looking for is not in the regs, so we are quite pleased by that. Setting up contracts with individual business partners of which for example, wearing my ENVOY affiliate hate right now, ENVOY has thousands of business partners. And it becomes quite unclear whether or not those business part-

ners have to execute contracts with ENVOY, of which there are thousands or tens of thousands, providers, pharmacies, payers, et cetera, et cetera.

Mr. MCDERMOTT. When you get that data, you guarantee that no one can unscramble your encryption and get out names or anything else, or mailing lists for anything?

Dr. OBER. It is as secure as anything that is technologically available, is what I can rest assured on.

Mr. MCDERMOTT. I really find it hard to understand why you are here, what you are worried about. If you are not exposing individuals in the society—

Dr. OBER. That is correct.

Mr. MCDERMOTT.—in any way, why should these regulations bother you? It is very curious to me. Maybe somebody else knows what he is worried about. I do not know. Ms. Goldman, do you have an idea?

Ms. GOLDMAN. I am heartened actually to hear that he supports essentially the draft regulation, which I think is important. Because if the description is accurate, that what ENVOY is transmitting is de-identified, it is then not covered by the regulation at all. The transmission of that information is then not covered because it is de-identified.

Mr. MCDERMOTT. Thank you for your indulgence for an extra 20 seconds.

Chairman THOMAS. One of the values of this testimony, I think, beyond doubt, especially your somewhat incredulous belief that there was some value in whatever it was that these folks did from a business point of view—I was curious whether they were publicly held and how much they were selling this stuff for—is just an indication of how much is going on out there that even knowledgeable people may not be familiar with, but if you say something that sounds innocuous, business entities must and therefore in extension with other business partners create relationships in which you may have had no intention whatsoever of disrupting, but in fact you may very well.

His initial statement, the description of what they do, the fact that someone believes there is value in it, and that they would have to then comply with everybody else who may or may not be identified as business partners, I think he has every right to be concerned about how HCFA in the reg does identify business partners, notwithstanding the content being de-identified. I doubt if, in fact, it was going to get into de-identifying public partners in terms of the data they have versus identified public partners in the data that they have, versus those that are merely transmitters of that data from someone else.

It is that kind of complexity that is out there today producing value that people are willing to spend literally millions of dollars for that may, in fact, be significantly disrupted. That is the concern we have. I appreciate the gentleman taking valuable time out of doing whatever it is you do that people think is really valuable, for however much it is worth, to sensitize us to the concerns that you have.

The gentleman from Maryland?

Mr. CARDIN. Thank you, Mr. Chairman.

Of course, if we had given HHS proper authority or delegation or if we had passed a bill, we would not have this problem. I think the only reason we have this convoluted process is because of the desire of HHS to have an enforceable privacy act and under the HIPAA statute they do not have the ability to do it. That is why we need to enact a bill.

Chairman THOMAS. I obviously totally agree with the gentleman but I do hope that people understand that, by that inference, I do not think that you mean that the HIPAA legislation was designed to be perverse or to create a structure which would, in anticipation, create the problems?

Mr. CARDIN. No, I think we anticipated that Congress was going to pass a privacy act, and we have not done that.

Chairman THOMAS. Exactly.

Mr. CARDIN. All these are trade-offs. It is interesting, you talk about the trade-offs for privacy for the patient versus the need for information to be available for good purposes, whether it be law enforcement, whether it be research, or whether it be treatment. And there is trade-offs on cost. Every time we put additional requirements in to protect privacy, there is going to be some sacrifice of efficiency. So it is going to be all trade-offs.

I want to just concentrate on one, which we affectionately call the statutory authority, or when the identifiable information can be made available without the specific authorization of the patient. If I understand Ms. Goldman's point, you are concerned that in the regulation the use of that information should be signed off by the patient. That is the patient gives specific authorization, but must know that information can be made available by signing off on a form indicating an acknowledgement of that. Is that correct?

Ms. GOLDMAN. Exactly. It essentially makes the notice requirement that is currently in the proposal more meaningful. Right now, the way the health care system operates is that people do not get care or enroll in a health plan unless they sign an authorization form. People sign at the point of care and the point of enrollment right now. The Secretary is proposing not only eliminating that practice but prohibiting that practice for the sharing and collection of information.

It is not necessarily a meaningful requirement right now in current practice, in other words you do not have a real choice about withholding your authorization. But it does, I think, alert the public to how their information is being used and who might get access to it.

Mr. CARDIN. I certainly agree that notice should be given to patients. Patients should absolutely know that. My concern is what happens if the patient does not sign off on the acknowledgement?

Ms. GOLDMAN. My understanding of the way the current system operates is that you can withhold treatment and deny benefits if people do not authorize the use and disclosure of information for treatment and payment. And right now, they are authorized to release the information for a broad category—

Mr. CARDIN. There is broader reasons than just treatment and payment. I guess my question is if the patient does not sign off on the acknowledgement, or if the user does not have a copy of that in the file, what does that mean?

I think we have to think that ought. Clearly, I agree with you, notice is absolutely essential, that the person understands what the information can be used for. I just do not know whether signing off is the right way to do it, and whether that does not just create more problems for Ms. Fox and Ms. Grealy on administrative costs.

Dr. Plested, I want to just follow up, so I understand the AMA's position, because you have a narrower interpretation of what should be allowed. You want to have more specific authorization from the patient. I take it not in regards to treatment? Or is it in regard to treatment, also?

If you get a request from a physician who you have referred a patient to, can you make that medical information available without a specific authorization, under your position?

Dr. PLESTED. Clearly, if we have had a referral from another physician and the patient comes to see us, I think there is an implied consent that we share the information about that patient.

Mr. CARDIN. So you would not need specific authorization for that?

Dr. PLESTED. No.

Mr. CARDIN. How about paying a bill? Would you require specific authorization for that?

Dr. PLESTED. This gets a lot tougher. Because what information is needed to pay a bill? Today, if I submit a bill for a consultation, I have to submit the full consultation to the insurer. Why does the insurer need to know your mother's family history or what your sexual preference is, or anything else, because I saw you because you have a sore foot?

Mr. CARDIN. That is fair enough, I agree with you. It should be related to the need for payment.

Dr. PLESTED. That is right. But now the insurer has a form signed that he gets everything, and I cannot get paid without it.

Mr. CARDIN. That is specific authorization in most cases today. The problem we have, and I think Ms. Goldman mentioned it, routinely when a person signs up for a health care plan they sign a lot of forms. In many cases, they do not even know what they are signing. And they are giving blanket authority right now to release everything.

At one point we are going to have to talk about the use of specific authorization. But I think what HHS is trying to achieve, and I know what Mr. Thomas is attempting to do, is to have reasonable statutory authority specifically as to what information is really needed so that we get away from these blanket authorities, so that we get away from people not knowing that they have released so much information that is unnecessary, because your point is well taken. The doctor should not have to submit the whole family history for payment.

And if we have proper statutory authority, I would submit, that would not be happening. But because of the absence of statutory authority in this area, we find that there is more information being made available through specific authorization than is needed.

Dr. PLESTED. And if I could continue that, that goes directly to the Chairman's question about whether we have a floor or a preemptive rule, and it depends on where the bar is. If the bar is high like you suggest to protect patient's privacy for only that informa-

tion that is absolutely necessary, the AMA says yes, we will look at a Federal preemption.

But now the Secretary's bar is so low, protecting the patient and giving any entity outside all the information that they want, that is why we feel that stronger state laws are important.

Mr. CARDIN. Thank you, Mr. Chairman.

Chairman THOMAS. Thank the gentleman. I want to thank all of the witnesses and the members. Another question? Go ahead.

Mr. MCDERMOTT. I appreciate your letting me ask one more question.

Chairman THOMAS. I reserve the right to thank all members.

Mr. MCDERMOTT. I want to go back to Dr. Ober. The Quintiles 1998 report states that by combining services and connections and information ''Quintiles is creating on the Internet a unique software bridge of information between pharmaceutical products, patients, physicians, payers and regulators.''

Now, they do clinical trials?

Dr. OBER. Correct.

Mr. MCDERMOTT. So they have somebody's name then; correct?

Dr. OBER. I am sorry, sir?

Mr. MCDERMOTT. They have somebody's name then, when they are doing a clinical trial?

Dr. OBER. For clinical trial purposes they certainly, they would have the names at the physicians' clinical site, but everybody is blinded, to the best of my knowledge, to information that is centralized. The clinical trial results in many, many sites worldwide. Where an individual would collect, through case report forms, a variety of critical information about the study at hand.

Mr. MCDERMOTT. So Quintiles never receives anybody's name, ever?

Dr. OBER. No, I cannot make that statement, sir. Actually, our informatics group does not work with the clinical trials group at all.

Mr. MCDERMOTT. But you are all connected in this business relationship in your picture here; right?

Dr. OBER. Not Synergy, sir. Not ENVOY. The clinical trials capability, if you will, which is emerging for administrative efficiency to take place over the Internet and other interactive connectivities, is not part of the core business of the informatics group at all.

Mr. MCDERMOTT. But you are all business partners, by the definition of this rule and regulation; correct?

Dr. OBER. Okay, well, business partners with respect to the fact if we were using that information, which we are not. We have nothing to do with the clinical trial site of Quintiles. It is a separate entity.

I know the diagrams can be misleading, but there is no relationship at all between the clinical trials group and the information they collect is completely different information for very specific clinical purposes, which I believe is outside the reg, as opposed to what we are doing with de-identified information at Synergy and the informatics group. Completely different datasets.

Mr. MCDERMOTT. We have the wrong guy here. We should have the guy from Quintiles, as to whether he lets the information go over to the commercialization under Inovex, right?

Dr. OBER. I can assure you that there is no connection between patient names going from clinical trails to Inovex. That I can assure you of, sir.

Mr. MCDERMOTT. Thank you, Mr. Chairman.

Chairman THOMAS. As they usually say, this prospectus is for information only and it should not be considered to be legal. They have a whole lot of papers on file, and you are working off of one little picture here.

It is very complicated and if they have any clinical trials worth their salt, they are usually double-blind at the time of the clinical trials.

Dr. OBER. That is exactly correct.

Chairman THOMAS. Let alone with the transmittal of information.

I thank the gentleman very much.

I also thank all of you and, as I intended to say initially, this is a very difficult area. I appreciate everybody keeping the politics down to a minimum and, in fact, very visible because the policy is tough enough standing on its own.

Thank you very much and I look forward to working with you as we move forward. The subcommittee stands adjourned.

[Whereupon, at 12:43 p.m., the hearing was adjourned.]

[Submissions for the record follow:]

Statement of the American Academy of Pediatrics

The American Academy of Pediatrics was pleased to comment on the November 3, 1999 Notice of Proposed Rules on Standards for Privacy of Individually Identifiable Health Information. The Academy and its 55,000 members support the goal of protecting the privacy of identifiable health information. These proposed regulations are an important first step. However, because the Health Insurance Portability and Accountability Act of 1996 gives the Department of Health and Human Services only limited authority in this area, federal legislation protecting the privacy of all identifiable health information used by all entities is still necessary.

Our comments address many provisions of the proposed regulations. In particular, we would like to highlight the following:

1) Adolescents have a unique need for privacy concerning the many sensitive issues they often face. In many cases adolescents will obtain health care only if they are guaranteed that their parents will not learn about it. The privacy regulations must protect adolescents' rights. Generally, the regulations create a "floor," preempting less stringent state laws on privacy of health information. However, the regulations have a "hole in the floor" since minors are not guaranteed that the federal regulations will preempt less stringent state laws concerning their confidentiality rights. The regulations should provide minors with a uniform privacy standard, must preserve health care providers' ability to treat adolescents confidentially and must ensure that minors and their parents are informed of their privacy rights.

2) Health care providers should not be held accountable if protected health information is used for prohibited purposes by the entities to which they disclose the information. Once the information has been transmitted responsibly to a legitimate entity for a specified purpose, its privacy should be the responsibility of the receiving party.

3) Privacy standards should apply to all identifiable health information, regardless of whether it has ever been electronically transmitted or maintained.

4) The scalable nature of the regulations is very important in preventing an undue burden for physicians and ensuring effective provision of health care.

5) The provisions regarding research require substantial revision and clarification to better direct Institutional Review Boards and privacy boards and so that responsible research into important health concerns is not hampered.

The full text of the AAP comments will be available shortly at "*http://www.aap.org*"

The AAP comments are also endorsed by the Association of Medical School Pediatric Department Chairs, the American Pediatric Society, and the Society for Pediatric Research

AMERICAN COLLEGE OF PHSICIANS-
AMERICAN SOCIETY OF INTERNAL MEDICINE
WASHINGTON, DC 20006–1834
February 17, 2000

Margaret Ann Hamburg, M.D.
Assistant Secretary for Planning and Evaluation
U.S. Department of Health and Human Services
Attention: Privacy-P
Room G–322A, Hubert H. Humphrey Building
200 Independence Avenue, SW
Washington, D.C. 20201

Re: *Comments on the Proposed Standards for Privacy of Individually Identifiable Health Information,* 45 CFR Parts 160–164, 64 Fed. Reg. 59917 (November 3, 1999)

Dear Dr. Hamburg:

The American College of Physicians-American Society of Internal Medicine (ACP–ASIM), representing 116,000 physicians who specialize in internal medicine and medical students, is pleased to submit comments in response to the Notice of Proposed Rulemaking (NPRM) issued by the Department of Health and Human Services (HHS) and published in the FEDERAL REGISTER dated November 3, 1999. ACP–ASIM is in a unique position to evaluate patient privacy legislation: our members represent the gamut of internal medicine, including both general internists and subspecialists engaged in the practice of internal medicine as individual practitioners, members of group practices, government employees, professors of medicine, and medical researchers.

Summary of Comments

- We support the flexibility that would reject a "one size fits all" approach in implementing the privacy provisions, and the "minimum necessary" standard;
- We support the way the rule deals with disclosure of protected health information for research purposes, protecting patient privacy without imposing undue burdens that would impede research;
- We support providing patients with the right to inspect, copy and amend their patient records, and requiring notice to patients of their privacy rights and of how their medical information might be used or disclosed;
- We support the provisions regarding public health activities, health oversight, and judicial and administrative proceedings;
- In general, we oppose allowing the use and disclosure of confidential medical records without individual authorization for treatment, payment and health care operations (as defined in the NPRM);
- We are very concerned that the provisions on business partners would be very difficult to enforce, create open-ended and unpredictable liability for physicians and are unduly burdensome;
- We believe the provisions concerning law enforcement are too broad and would violate privacy rights;
- The costs of implementing the proposed rule have been vastly underestimated and would have a disproportionate impact on small business; and
- Physicians, especially those in small practices, will be subject to disproportionate administrative burdens as a result of the proposed rule, and should be exempted from the most onerous provisions of the rule. Physicians, unlike some of the other covered entities, are already bound by ethical obligations to uphold confidentiality and privacy rights of patients.

General Comments

Confidentiality is increasingly difficult to maintain in this era of computerized record keeping and electronic data processing, faxing of patient information, third-party payment for medical services and sharing of patient care among numerous medical professionals and institutions. ACP–ASIM commends HHS for tackling this difficult and complex issue and for attempting to ensure protection of patient confidentiality without impeding or preventing access to data that is essential to the

efficient delivery of quality patient care and for medical, public health and health services research. Given the limitations on HHS's authority, the approach of trying to protect the information itself is understandable. We are concerned, however, that the proposal generally sweeps all covered entities together under the same complex regulatory framework. Individual physicians, governed by ethical codes of conduct and state professional disciplinary codes, are being lumped together with large institutional providers, health plans, and clearinghouses. Are there data to suggest that individual health care professionals are routinely and intentionally breaching confidentiality, or that patients fear that they are? Anecdotally, patients express concerns about health plans, organizations and institutions breaching confidentiality, not their individual physicians. Physicians are obligated to protect patient confidentiality, especially in light of the increased risk for invasion of patients' privacy from the computerization and electronic transmission of medical records. We are concerned that the rule, proposed as "a basic set of legal controls," might be viewed instead as all that is required of physicians, and could undermine the traditional ethical and professional obligations to uphold confidentiality. Moreover, the proposed rule does not cover entities that are more likely to wrongfully disclose and misuse confidential information.

The ACP–ASIM recognizes the need for appropriate safeguards to protect patient privacy, because trust and respect are the cornerstones of the patient-physician relationship and quality health care. Presence of trust, respect, and privacy create an atmosphere in which full disclosure of information from patient to physician can occur, enhancing treatment. Patients have a basic right to privacy that includes the information contained in their medical records. Medical personnel who collect health information have a responsibility to protect patients from invasion of their privacy. Patients need to be treated in an environment in which they feel comfortable disclosing sensitive personal information to a physician that they trust. Otherwise, they may fail to fully disclose conditions and symptoms, thereby reducing the effectiveness of treatment and perhaps seriously imperiling their health, or, they may avoid seeking care altogether for fear of the negative consequences that could result from a disclosure. Physicians have a responsibility to respect patient privacy first, except when doing so may result in serious harm to the patient or others, or when required by law. See ACP–ASIM Ethics Manual (Fourth Edition), Annals of Internal Medicine 1998, 128: 576–594). We are concerned that the NPRM goes too far in the direction of disclosure of protected health information without individual authorization; our concerns in this regard are set forth in more detail under the section dealing with "Treatment, Payment and Health Care Operations."

The NPRM is an important step in ensuring federal protection for the privacy of medical records and represents significant progress toward finding the right balance between the privacy rights of patients and the free flow of information that is necessary for the provision of effective and efficient health care services. The limited scope of HHS's authority pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, however, illustrates that comprehensive federal privacy legislation is needed. Because of the limitations imposed on HHS, too many burdens for compliance are placed on physicians. **While we are not suggesting that the medical privacy rule should not be applied to physicians, we do think that there should be a reexamination of the need for some of the provisions, as they would be applied to small physician offices. To the extent that small physician practices are not exempted from the provisions, HHS should apply them in the least burdensome fashion.**

Introduction to General Rules

ACP–ASIM supports the "scalability" approach taken in the NPRM, under which a "one size fits all" standard would be rejected for the implementation of the privacy provisions. It is critical that each affected entity be able to assess its own needs and devise, implement and maintain appropriate privacy policies, procedures and documentation to address its business requirements. Our members range from physicians working in solo practitioners' offices to multi-group practices to academic health centers, all of which have different needs and business practices.

ACP–ASIM also supports the stated general approach of the rule whereby protected health information (PHI) could not be used or disclosed by covered entities except as authorized by the individual who is the subject of such information or as explicitly provided in this rule. We disagree, however, with the actual approach taken by HHS whereby most uses and disclosures of an individual's PHI would not require explicit individual authorization (see discussion below).

Since Congress has not yet passed comprehensive confidentiality legislation, ACP–ASIM believes that special safeguards are needed to cover certain highly sensitive parts of a patient's medical record, such as HIV status,

mental health disorders, drug and alcohol-related problems, sexually transmitted diseases, sickle-cell anemia, sexual orientation, and other highly sensitive health information.

Treatment, Payment and Health Care Operations

Subject to limited exceptions for psychotherapy notes and research information unrelated to treatment, a covered entity would be permitted to use or disclose protected health information (PHI) without individual authorization for treatment, payment or health care operations. The proposal would actually prohibit covered entities from seeking individual authorization, unless required by State or other applicable law. **While ACP–ASIM recognizes that this proposal is intended to make the exchange of PHI relatively easy for health care purposes and more difficult for other purposes, we are very concerned that this approach would allow the use and disclosure of confidential medical records without the consent of the patient in extraordinarily broad circumstances.** The proposed rule allow records to be shared without limit throughout the health care system; the confidentiality of medical records can be set aside for almost any reason at all. This approach undermines the bedrock principle critical to the physician-patient relationship of informed consent, and will undercut traditional codes of medical ethics.

Confidentiality between the doctor or other health care professional and the patient is an essential component of high quality health care. Physicians must obtain informed voluntary consent from the patient before their medical information is disclosed for any purpose, except for appropriately structured medical research (see below) or as required by law. (ACP–ASIM Code of Ethics; "Confidentiality of Electronic Medical Records," Public Policy Paper 2000). At some point in the treatment relationship between the patient and the physician, preferably at the first encounter, there should be some type of signed written authorization that is a legal, informed consent to the release of PHI for treatment and payment purposes. ACP–ASIM supports the approach taken in S. 578 (Jeffords-Dodd), e.g., some form of consolidated authorization by which health care providers and organizations can perform their various functions without having to stop and obtain authorization at every point in a patient's treatment. Consent is particularly important since the proposal generally would not restrict to whom disclosures could be made for treatment, payment or operations. When disclosures are made to non-covered entities (other than business partners), the protections afforded by this rule would not be applicable. While this limitation points to the need for passage of more comprehensive privacy legislation, until such legislation is passed, individual's health information must be protected more strongly than provided under the NPRM.

Likewise, allowing disclosure of PHI without authorization for health care operations is problematic, given the broad definition of "health care operations." **As indicated above, ACP–ASIM supports requiring authorization before PHI can be used or disclosed for most health care operations. At the very least, the definition of what is considered to be health care operations should be narrowed to include only those activities that truly are related to treatment or payment.**

Minimum Necessary

ACP–ASIM agrees with HHS that a covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure. Access should be limited to only those individuals who need access to the information to accomplish the use or disclosure. De-identified patient data should always be used in medical research and quality improvement processes, unless the nature of the research necessitates identification because coded data would be impracticable.

We support the use of firewalls to limit the possibility for improper data uses within an entity, but note that the proposed scalability standard is particularly desirable in creating barriers to access and review of PHI. Physicians maintain records in a variety of settings, from large academic institutions to private offices with two staff members who perform all administrative functions. Current conditions in medical offices typically place physical barriers between medical records and non-staff, as well as limiting business partners' access to records.

Practice management software and electronic medical record software packages are widely used by health care providers. Privately owned physician offices have limited access to technology with the capacity to create firewalls within their offices. Although software packages are available with a wide range of customizable features, they typically do not limit access on a field-by-field basis. Many programs limit access on a screen-by-screen basis or a function basis (such as appointment

scheduling, billing, viewing laboratory results), but these are not completely customizable. Purchase of custom programming or replacement of current computer systems would represent an undue burden on providers who currently have as little as $300 or as much as $50,000 invested in computer software. Encryption technology is not currently available to most small businesses.

Proposed §164.506(b) generally would place the responsibility for determining what is the "minimum necessary" disclosure on the covered entity making the disclosure. Covered entities would be required to make "reasonable efforts" and to incur "reasonable expense" to limit the use and disclosure of PHI. This standard, while flexible, when combined with the scalability approach leaves a health care provider's staff with a large amount of discretion and complete liability. It is not clear what "reasonable" means in this context; there is much gray area between what is "necessary" information for medical reasons and what is too much disclosure. In addition, a covered entity would be required to review each request for disclosure individually on its own merits, rather than institute a policy to approve certain types of requests. This provision will require that an individual with authority and knowledge to make "minimum necessary" determinations must review each record request. In small practices, page-by-page review of multiple record requests on a daily basis could pose excessive administrative time requirements. In many cases, it will be cumbersome to determine the exact need for every piece of information and exact measurement of information that may be required to meet that need.

We would encourage HHS to reconsider the excessive requirements placed upon clinical staff by transferring the burden of responding to medical record requests from clinical staff to administrative personnel. Each hour of record review is deducted from the limited time that physicians and nurses are able to perform their primary functions, caring for patients. **Covered entities, particularly small businesses, should be allowed to create an internal policy to allow clerical staff to respond to many routine types of releases, including 1) disclosures allowed under any section of this proposed rule without patient authorization, and 2) any request accompanied by a written authorization signed by the patient. Moreover, the burden should be on the requestor of the information to make the "minimum necessary demand."**

Right to Restrict

ACP–ASIM generally supports the right of an individual to request that a covered entity restrict further uses and disclosures of PHI for treatment, payment or health care operations. However, administering a system in which some information is protected and other information is not poses significant challenges. In reality, this right will be severely hampered by health care providers' contractual obligations to insurers. Managed care organizations normally require that participating physicians not enter into private contracts for treatment and payment outside the physician's contract with the MCO. Thus, in its practical application, this right may be restricted to self-pay patients.

In cases not involving reimbursement, such as release to other physicians, providers may make good faith efforts to avoid those disclosures, but implementing security systems and tracking those limitations will be extremely difficult due to systems limitations. Electronic systems do not provide the capacity to exclude transmissions to particular providers. Physician office groups may request paper records and administrative staff may be unaware of the affiliation of a particular provider within that group. Tracking a myriad of restrictions may be impractical and could result in denial of all requests to avoid disclosure liabilities. **We would support providing examples in the final rule of appropriate, scalable systems that would be in compliance with this proposed provision.**

The Preamble notes that the proposed rule would not require a covered entity to agree to a request to restrict, or to treat or provide coverage to an individual requesting a restriction. HHS correctly recognizes that the medical history and records of a patient, particularly information about current medications and other therapies, are often very much relevant when new treatment is sought. Physicians have an ethical and in many cases legal obligation to treat a patient until that patient has been formally transferred to the care of another provider and/or discharged. **Provisions should be made to accommodate provider treatment and disclosure after the covered entity has refused a non-disclosure request.**

Creation of De-identified Information

ACP–ASIM supports the approach proposed in § 164.506(d) for de-identifying identifiable information and the use of restrictions designed to ensure that de-iden-

tified information is not used inappropriately. We believe that health information should be encrypted before being transmitted electronically for research purposes. For the majority of physicians in private practice, however, development and implementation of procedures for stripping identifiers will be cumbersome. A typical physician's office has neither the technical ability to create de-identified data nor the staff to manually de-identify data. **We support a "reasonableness" standard whereby entities with sufficient statistical experience and expertise could remove or code a different combination of information.**

Business Partners

We have major concerns with and strongly object to the business partner provisions. While we recognize the limitations imposed on the authority of HHS to directly regulate entities other than health plans, health care providers and clearinghouses, we are concerned that under the business partner provisions, physicians would become regulators for HHS. These provisions would not only be unduly burdensome to physicians, but also would be exceedingly difficult to enforce. Physicians would be exposed to open-ended, unpredictable liability. Each of these concerns is discussed in further detail below.

Under the proposal, for purposes other than consultation or referral for treatment, covered entities would be able to disclose PHI to business partners only pursuant to a written contract that would limit the business partner's uses and disclosures of PHI. The contract between the covered entity and the business partner would be required to include certain provisions that are specified in the proposal. Each specified contract term would be considered a separate implementation specification under the proposal, and a covered entity would be responsible for assuring that the business partner meets each such implementation standard. These complex contract terms and new obligations will necessitate the investment of much more time and resources by medical and legal personnel. Business partners may incur substantial expenses in meeting privacy requirements, which could result in more expensive contracts for health care providers.

Non-compliance by a business partner or its sub-contractor of the terms of the contract could expose the physician to significant civil or criminal sanctions. Physicians would be in violation of the rule if they knew or "reasonably" should have known of a material breach of the contract by a business partner and failed to take reasonable steps to cure the breach or terminate the contact. Physicians would also be responsible for mitigating the harm caused by such violations. It will be very difficult, if not impossible, for most physicians to enforce the required contracts. No analysis has been done of the number of single-source business partners used by health care providers. A Medicare carrier acting as a fiscal intermediary, for example, would qualify as a business partner. However, HHS awards single-source contracts, leaving the physician with no viable alternative if required to terminate a contract. **These provisions, by making physicians liable for disclosures by others not under their control, raise serious questions of fairness, and should not be included in the final rule.**

Business partners will be impacted by the need to maintain business records for legal and/or financial auditing purposes. This may make the destruction or return of all PHI unlikely or impossible in certain circumstances. For example, billing services are subject to HHS audit. If business partners cannot maintain PHI, they cannot provide documentation of coding or submissions material, nor protect themselves from claims made against them related to bookkeeping errors. Computer back-ups that are maintained by many business partners might include PHI. Business partners cannot be expected to destroy all forms of electronic back-up just because they have completed work for one particular client. Outside entities that provide financial services and have access to information included on standard explanation of benefits forms will also be required to identify and destroy substantial numbers of documents. Such entities could include banking entities providing lockbox services, billing services, third-party medical collection agencies, third-party coding experts, consulting and auditing services and third-party claims processors, such as Medicare carriers.

Finally, and perhaps of most concern, a requirement included in the proposed contractual agreement would create a private right of action. Individuals whose PHI is disclosed by a business partner in violation of the rule would be considered to be third-party beneficiaries. As a third-party beneficiary, a patient would have a right under contract law to enforce the terms of the agreement by seeking damages against the breaching business partner and against the covered entity for failure to select and monitor properly the business partner. Covered entities would most likely have to purchase a rider under their insurance policies in order to be covered against such claims.

Uses and Disclosures with Individual Authorization

The regulation would require that covered entities have authorization from individuals before using or disclosing their PHI for any purpose not otherwise recognized by this regulation. ACP–ASIM supports the requirement that individuals must give specific authorization before a covered entity could use or disclose PHI for purposes unrelated to health care treatment or payment. (As discussed earlier, ACP–ASIM opposes disclosure of PHI without patient authorization except in limited circumstances).

We support the provisions in this section. Physicians must release information to the patient or a third party at the request of the patient. (ACP–ASIM Ethics Manual) Patient-initiated authorizations should be specific enough in terms of the information to be disclosed and to whom the information is to be disclosed to enable the physician to comply with the individual's request. Specific authorization is much better than the current practice of using broad disclosure forms. **ACP–ASIM supports requiring an expiration date as well as allowing authorization to be revoked by a patient unless action has been taken in reliance on the authorization.** With respect to authorizations initiated by covered entities, we support the requirement that the authorization form should identify the purposes for which the information is sought as well as the proposed uses and disclosures of that information. Patients need to be able to make informed decisions. Finally, we support the provision stating that treatment and payment should not be conditioned on a patient's authorization.

Public Health Activities

ACP–ASIM supports the provisions that would permit covered entities to disclose PHI without individual authorization to public health authorities carrying out public health activities authorized by law, to non-governmental entities authorized by law to carry out public health activities, and to persons who may be at risk of contacting or spreading a disease. Confidentiality may be overridden to protect the public health or individuals such as sexual partners at risk, or when the law requires it (e.g., mandatory public health reporting). However, before breaching confidentiality, physicians should make every effort to discuss the issue with the patient. (ACP–ASIM Ethics Manual).

Health Oversight

ACP–ASIM supports allowing disclosure or use of PHI without individual authorization for health oversight activities. **However, individual identifiers should be coded or encrypted whenever practicable.**

Judicial and Administrative Proceedings

ACP–ASIM supports permitting covered entities to disclose PHI in a judicial or administrative proceeding if the request for such PHI is made through or pursuant to an order by a court or administrative tribunal. A court order would not be required if the PHI being requested relates to a party to the proceeding whose health condition is at issue, and where the disclosure is made pursuant to a discovery order or is otherwise authorized by law. In the latter instance, however, we are concerned that the burden and possible liability is on physicians to determine whether the request relates to the PHI of a litigant whose health is at issue. Physicians and their staff are not best suited for making such determinations.

Law enforcement

The proposed rule would permit covered entities to disclose PHI without individual authorization to a law enforcement official conducting a law enforcement inquiry authorized by law if the request for PHI is made pursuant to a judicial or administrative process. We think that these provisions are too broad. Access by law enforcement officials to individual health records constitutes an inherent privacy violation. Health information is collected to provide quality care to patients and to help society through use of data in public health research. This information is not intended for law enforcement because of the potential for abuse. Access by law enforcement agents should be restricted to searches that are not open-ended and for which there is a just cause. **Release of confidential medical records to law enforcement officials should be permitted only when sustained by either subpoena or court order, except in limited emergency circumstances. Broad-based access is not an acceptable option. Law enforcement should be required to go through an independent review or neutral magistrate.** Administrative subpoenas may be issued based on an individual law enforcement request, sometimes

without any higher review. **HHS should require that law enforcement officials obtain a judicial order**

Research

It is critical that the provisions dealing with research recognize the precarious balance between protecting patient privacy and expanding on our knowledge of health and disease. Rules need to be structured so that they will not unduly burden health researchers in their quest to further public health and other vital medical research.

We generally support the way the proposed rule deals with research and the privacy of patient information. The proposal would permit covered entities to use and disclose PHI for research without individual authorization, provided that the covered entity receives documentation that the research protocol has been reviewed by an institutional review board (IRB) or equivalent body, and that the board found that the research protocol meets specified criteria designed to protect the subject. Absent such documentation, the subject's PHI could be disclosed for research only with the individual's authorization.

IRBs review research requests to ensure adherence to standards of patient protection and treatment in medical research. The boards are established to ensure that patients have been fully informed and that they have consented to their participation in clinical research. Any research using patient information—whether the information is identified or not, whether consent is obtained or waived—should be approved by an IRB. IRBs are an efficient and effective way to protect the rights and privacy of patients who consent to sharing their health information for the benefit of medical research. The conduct of research and the protection of patient confidentiality also must be in compliance with professional ethical guidelines and codes of conduct.

De-identified data should be used in medical research whenever possible, unless the nature of the research necessitates identification because coded data would be impracticable. All medical research studies that use potentially individually identifiable information must contain measures to protect the confidentiality of individual patient records and should be examined and approved in advance by an IRB or similar ethics review board.IRB functions include carefully reviewing the type of patient consent needed within the context of each study. Additional protection for subjects should be required if the information is identified and the waiver of consent in these instances should be limited.

The use of data sets for secondary research studies should be allowed for statistical analyses and public health, but the records should remain encoded whenever possible. Patients, however, should be notified when information is to be used for purposes other than originally agreed on, and they should have the option to deny consent. These other purposes include billing, organizational research and quality improvement programs. Unfortunately, there is no clear line to differentiate between a routine use and a research use. Often, primary and secondary data uses overlap, and their definitions are dependent on the context within the individual studies. Uses of "de-linked" information require review by an IRB or other similar panel. While we recognize the limited authority of HHS over researchers who are not covered entities, **the ACP–ASIM believes that the burden for information requests should be borne by those requesting access to the information; we realize the need for stringent review in determining who has access to de-identified information.**

Notice of Information Practices

We generally support the provisions in this section that would require health plans and providers to give notice of their confidentiality practices and procedures to patients. Such notice would be intended to inform patients about what is done with their PHI and about any rights they may have with respect to that information. Notice is an essential component of giving individuals the ability to make informed choices about their medical treatment. **We support a flexible approach in allowing each provider to create a notice that reflects its own unique information practices.**

We do have concerns, however, about the administrative burdens and costs of such requirements, particularly for small practices. Small businesses are required to provide a notice of information practices on the patient's date of first service after the effective date of the rule. Determining the "first service" would place an undue administrative burden on many small practices. On a daily basis, staff would have to manually review each chart, or, in many cases, access a computer system to determine whether the patient has been seen since implementation of the rule. Inter-

nal medicine physicians average 4,000–5,000 patient charts; approximately 2,200 charts are considered to be "active." ("active" should be defined as those patients who have been seen in the last two years) The initial cost to produce, copy and mail notices could easily exceed the estimated $375 first year cost per provider office. Assuming 50 cents per authorization, the total cost could easily reach $1100 per provider in medical offices. Moreover, the cost attributed to tracking individual patient receipt of the notice would be extensive. These administrative costs would be incurred again whenever a notice is updated. **Physicians who mail notices to active patients, prominently display the notice and provide the notice to all new patients should be relieved of any additional notification requirements.**

Requiring signed acknowledgment of the notice, which in theory sounds like a good practice, in reality will only increase administrative burdens and costs. We also suggest a clarification to the provisions. The proposal does not clearly define the scope of initial notifications required. Will notification be required if the patient's last treatment date was prior to the rule's effective date?

Access for Inspection or Copying

Patients have a legal and ethical right to review information in their own medical records. In rare and limited circumstances, health information may be withheld from a patient if there is significant likelihood of a substantial adverse effect on the physical, mental or emotional health of the patient or substantial harm to a third party. The onus is on the provider to justify the denial of access.

The proposed rule would allow, but not require, a researcher/provider to deny a request for inspection and copying of the clinical trial record if the trial is still in progress, and the subject-patient had agreed to the denial of access in conjunction with the subject's consent to participate in the trial. The IRB or privacy board would determine whether such waiver of access to information is appropriate, as part of its review of the research protocol. In the rare instances in which individuals are enrolled in trials without consent (such as those permitted under FDA regulations), the covered entity could deny access to information during the course of the trial even without advance subject consent. However, access during the trial would be appropriate if a participant has a severe adverse reaction and disclosure of information during the clinical trial would give the participant adequate information for proper treatment decisions. In all cases, the subject would have the right to see the record after the trial is completed. We agree with these provisions.

Access to current records within thirty days is reasonable for active patients. Medical records of patients last seen more than two years previously, however, may have been moved to off-site storage, which necessitates a longer recovery period (perhaps 60 days), and incurs additional cost. **We suggest that a structured extension procedure should be included in the final rule. We do not support requiring an acknowledgment procedure.**

Accounting of Disclosures

While we support in principle the requirement for an accounting of disclosures, we have several concerns about the proposal in its current form. First, covered entities would be required to provide an accounting of all instances where PHI is disclosed for purposes other than treatment, payment and health care operations. However, as currently drafted, PHI may be disclosed without individual authorization for those purposes. Thus, patients could learn who has had access to their PHI only when such information is disclosed with their consent, but they do not have such a right when consent has not been given. It would seem that it would be more important to provide an accounting for disclosures where an individual has not given prior authorization.

Second, we are concerned about the administrative burden and cost of complying with the accounting requirements. We agree that accounting should not be required for payment, treatment and most health care operations, but, as discussed earlier, we recommend that individual authorization should be required prior to the disclosure or use of PHI for such purposes.

Finally, we suggest amending section 164.515(c)(1)(v) to clarify that "copies of all requests for disclosure" refers only to individual-initiated requests.

Amendment or Correction

We support the right of patients to review the information in their medical records and to propose corrections. At the same time, however, it is critical to keep in mind that medical records provide working documentation for physicians and are often referred to in support of actions taken on the patient's behalf. The integrity

of the medical record is critical. Therefore, medical histories should not be re-written or deleted. Physicians are liable to health plans for providing supporting documentation for all information submitted and requests for payment. If this information is later determined to be inaccurate, corrections can be made and submitted as appropriate. The original documentation, however, is still necessary.

Training

Many health care providers' employee training programs or employee handbooks currently incorporate confidentiality policies, so the additional burden imposed by the initial training requirement would be negligible. Re-certification, however, would impose a new administrative burden and is of questionable value when privacy policies remain unchanged. *Re-certification should be required only when a provider's privacy policy significantly changes.*

Safeguards

The proposal would require that a covered entity have appropriate technical and physical safeguards to protect the privacy of PHI. Medical records intermingle electronically transmitted data, non-electronically transmitted data, and data that is referenced in both formats. Therefore, providers most likely will have to presume that all records must be considered PHI and treated as such. Many small practices keep records in central areas easily accessible to all staff; such areas are not easily adaptable to "locked storage" areas. Replacement of an open medical chart storage cabinet with a lockable unit costs approximately $800 and provides little benefit. A typical physician has between three and ten units. **A small business should be required instead to provide physical barriers (e.g., walls or counters) to limit the access of non-authorized personnel to record storage areas.**

The proposal also would require a covered entity to verify the identity and/or authority of persons requesting PHI. This places an unusual burden on health care providers to verify requests that are normally received verbally or via fax. Moreover, ascertaining whether a requestor has the appropriate legal authority is beyond the scope of the training or expertise of most employees in a physician's office. **Health care providers must be able to reasonably rely on the authority of the requestor.**

Sanctions

We support the flexibility in the proposal that would allow covered entities to develop the sanctions policies appropriate to their businesses and operations. The ACP–ASIM supports holding users of electronic medical data accountable for protecting patient privacy. We are concerned, however, that a provider would be held liable for violations by a business partner and its subcontractors. As discussed earlier, *we think that there are fundamental fairness issues in holding providers accountable for the actions of another entity that they do not control.*

Small Business Impact

The NPRM does not propose a specific definition for small businesses, but incorporates the U.S. Small Business Administration's (SBA) baseline revenue definition for small businesses, which is $5 million in annual revenue. We do not believe that this proposed guideline, as currently defined, will include the projected 90% of health care providers. The Medical Group Management Association's Cost Survey Report for 1998 indicated that only 52.01% of group practices would not exceed the $5M revenue threshold. In addition, the SBA has proposed adjusting the revenue requirement for Doctors of Medicine (SIC 8011), as well as certain other health care-related providers, to $7.5 million. SBA has proposed this increase to reflect the disadvantage that health care providers face in a highly competitive market, even though their revenue has increased. We would encourage HHS to reflect this amended revenue standard in the final rule.

Additionally, we encourage HHS to consider establishing an alternative test for small businesses, based upon number of employees. Health care providers in particular areas of medicine, such as cardiology or oncology, would exceed the revenue requirements in a practice of four to five physicians. To achieve parity across specialties with widely divergent average revenues, we encourage HHS to consider extending the definition of small business to any health care provider employing less than twenty employees. **This definition is supported by the report, "Employer Firms, Employment, and Estimated Receipts by Firm Size and Industry, 1996," issued by the SBA's Office of Advocacy, which indicates that 92% of Doctors of Medicine worked in firms with fewer than 20 employees.**

Conclusion

The proposed rule is an important first step in ensuring federal protections for the privacy of medical records. The ACP–ASIM appreciates your consideration of our comments and looks forward to working with you as the rulemaking process continues. If you have any questions, please do not hesitate to contact Debra Cohn, Legislative Counsel (202/261–4541) or Jack Ginsburg, Director of Policy Analysis and Research (202/261–4542).

Sincerely,

WHITNEY W. ADDINGTON, M.D., FACP
President

AMERICAN COLLEGE OF SURGEONS
WASHINGTON, DC 20007
February 16, 2000

The Honorable Bill Thomas
Chair, Subcommittee on Health
Committee on Ways and Means
U.S. House of Representatives
1136 Longworth House of Building
Washington, DC 20515

Dear Chairman Thomas:

As you and members of your Subcommittee prepare to examine the extraordinarily complex issue of medical records confidentiality, the enclosed copy of the College's response to the Department of Health and Human Services (HHS) proposal on this issue may be useful.

In its comments, the College recognizes the enormously difficult task the HHS Secretary faced when drafting this proposed rule, and we commended the Department for its effort to generate regulations that are consistent with sensible health information confidentiality principles. However, we believe strongly that the proposed rule overreaches its mandate in some areas, fails to take into account important private-sector activities that contribute to high-quality patient care, and imposes unreasonable burdens on physicians and their staff. Therefore, the College still believes that strong federal legislation is needed to provide a more tightly drawn blueprint for federal regulations.

Some of our key concerns with the proposed rule, described in more detail in the enclosed text, can be summarized as follows:

- The list of covered entities included in the proposal does not adequately account for the wide range of those that contribute to the modern, integrated health care system. As an example, it is impossible to determine how the College's own centralized cancer registry, the National Cancer Data Base, would be treated and what requirements it would need to meet.
- Improvements can be made in the definitions that were developed for "treatment," "payment," and "health care operations." In particular, we question how much patient identifiable information is necessary for fraud and abuse detection and compliance programs, or for general evaluation of provider performance.
- The mandate that covered entities adhere to a "minimally necessary" requirement when disclosing protected health information should be modified to provide more explicit guidance. Further, we suggest that entities requesting protected information should bear greater responsibility for determining the minimum amount necessary to complete their efforts.
- The College vigorously objects to provisions that would essentially require covered entities to be knowledgeable about and adhere to the information policies adopted by the whole assortment of businesses with which they are partners. We believe that HHS has greatly overstepped its statutory authority in this provision, and recommend that the standards be modified to require only that physicians and other covered entities make reasonable efforts to enforce their contracts; they should not be held responsible for their business partners' transgressions.
- The list of data elements that would need to be stripped from the medical record to be considered "de-identified" is far too sweeping and, if implemented, will render the record unusable for many types of medical research and disease surveillance registries.
- The definition of health oversight agencies allowed access to patient information appears to include only those that are government-based. Other key, private sector

organizations, such as the Joint Commission on Accreditation of Healthcare Organizations, are not granted equal privileges. Indeed, the College conducts programs that rely on patient data to assess and approve hospital-based cancer, trauma, and burn programs—these programs simply could not operate under the restrictions being proposed by HHS.

- To increase the odds of patients understanding of the notices they receive about a provider's information practices, HHS should reconsider its decision to abstain from developing a uniform format. The more patients see similar documents, the less likely they are to become disoriented when examining a new notice, particularly when presented with multiple notices for an episode of care that involves more than one provider.

Finally, as we note in our comments, many of the problems encountered with current patient information management practices result from the patchwork of state laws that complicate our increasingly interstate health care delivery and financing systems. We urge Congress to enact legislation preempting all state laws and establish a single, national standard for the care and management of patient medical records.

The College welcomes the Subcommittee's interest in addressing this remarkably complicated and important issue. We hope that you will call on us to assist in your efforts to develop reasonable, workable legislation to resolve the many difficult issues involved, including those problems that arise from the Secretary's limited regulatory authority in this area. Please do not hesitate to contact Christian Shalgian in our Washington Office, at (202) 337–2701, if we can be helpful.

Sincerely,

THOMAS R. RUSSELL, MD, FACS
Executive Director

[An attachment is being retained in the Committee files.]

Statement of the American Council of Life Insurers

I. INTRODUCTION

The American Council of Life Insurers (ACLI) is a national trade association whose 435 member companies represent 73 percent of the life insurance and 86.9 percent of the long term care insurance in force in the United States. The ACLI also represents 71 percent of the companies that provide disability income insurance. The ACLI is please to submit a summary of its comments on the proposed Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 through 164, (the proposed rule) promulgated by the Department of Health and Human Services (Department). The entire text of the ACLI's comments can be found on our public web site at ACLI.com.

The ACLI supports the goal of the Department of Health and Human Services (Department) to protect the privacy of individually identifiable health information and supports implementation of the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (P.L. 104 − 191) (HIPAA). Life, disability income, and long term care insurers understand their responsibility to protect individually identifiable health information. ACLI member companies are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their medical information and that insurers have an obligation to assure individuals of the confidentiality of that information.

Two years ago, the ACLI Board of Directors adopted the "Confidentiality of Medical Information Principles of Support." The ACLI has just amended these Principles to strengthen them even further to provide for support for prohibitions on the sharing of medical information for marketing and for determining eligibility for credit. A copy of the Principles is attached to this statement. Life, disability income, and long term care insurers have a long history of handling individually identifiable health information in a confidential and appropriate manner and are proud of their record as responsible custodians of that information.

The ACLI strongly supports the Department's fundamental goal of protecting individually identifiable health information. We believe that the Department can pursue this goal in a manner consistent with the public interest in maintaining life, disability income, and long term care insurance markets which meet the private insurance needs of American consumers. By their very nature, the businesses of life, disability income, and long term care insurance involve personal and confidential relation-

ships. However, insurers selling these lines of coverage must be able to obtain and use their customers' individually identifiable health information to perform legitimate insurance business functions, essential to insurers' ability to serve and fulfill their contractual obligations to their existing and prospective customers. We have analyzed the proposed rule with a view to balancing the goal of protecting the confidentiality of individuals' individually identifiable health information with life, disability income, and long term care insurers' need to obtain and use that information in order to issue, service, and administer insurance policies sought by individuals.

We were pleased that Secretary Donna Shalala, as the Keynote Speaker at the ACLI's Annual Meeting in November of 1997, acknowledged the importance of access to individually identifiable health information to the ability of insurance companies to provide the essential protection that only private insurance affords. Secretary Shalala stated: "I know that you support confidentiality legislation as long as it doesn't jeopardize your ability to underwrite in a fair and fiscally prudent manner and to evaluate claims." This statement by the Secretary is a trenchant declaration of the fundamental point of this letter.

It is important that the Department understand and consider all of the possible results of the proposed rule on covered entities and other entities that will be impacted by it. We are concerned that the proposed rule fails to take into account its impact on entities that are not covered entities, but which would be significantly impacted by the rule, particularly life and disability income insurers. We are also concerned that the proposed rule does not adequately take into account its impact on insurers which sell long term care insurance which are currently directly subject to the proposed rule.

Appropriately, insurers selling life insurance are not covered entities subject to direct regulation under the proposed rule. However, life insurers must obtain protected health information, essential to underwriting and claims evaluation, from doctors, hospitals, and others who may only disclose protected health information as permitted under the rule.

While it appears that disability income insurance policies are not intended to be health plans and that insurers which sell disability income insurance policies are not intended to be covered entities, this is not entirely clear. We believe that disability income insurance policies are not health plans, that disability income insurers are not covered entities, and that the proposed rule should make this clear. Also, as with life insurers, we are concerned with the proposed rule's impact on disability income insurers' ability to obtain from covered entities health information essential to underwriting and claims evaluation activities.

We are concerned by the proposed rule's inconsistency with HIPAA by virtue of its inclusion of a number of HIPAA "excepted benefits" within the definition of health plan, making insurers which sell these lines of coverage "covered entities." This appears to be contrary to Congressional intent to have the rule address comprehensive medical coverages only. It also appears contrary to the Department's intent as expressed in the preamble section "Definitions," in connection with the definition of health plan.

We are particularly concerned by the proposed rule's characterization of long term care insurance policies as health plans, making long term care insurers covered entities. For the reasons explained below, we strongly believe that this is inappropriate. Long term care insurance policies should be deleted from the list of coverages defined as health plans. If insurers which sell long term care insurance continue to be covered entities in the final rule, we would be very much concerned by the proposed rule's impact on their activities, as explained below.

There is also troublesome ambiguity in the proposed rule with respect to the obligations of an entity which is a covered entity for purposes of some of its activities and not a covered entity for purposes of other activities. A life insurer is not subject to the proposed rule as a covered entity. As the rule is currently drafted, a long term care insurer would be a covered entity. In fact, many life insurers are also long term care insurers. It does not appear to be the intent of the proposed rule to make the insurer a covered entity with respect to its use of protected health information in connection with life insurance, nor is there statutory authority to extend the rule in this manner. However, neither the rule nor the explanation in the preamble make this clear. The rule and the preamble should make clear that an entity involved in several lines of business, one of which is subject to the rule, will not be subject to the rule with regard to its other businesses.

II. INSURANCE AND THE ROLE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

The system of classifying proposed insureds by level of risk is called risk classification. It enables insurers to group together people with similar characteristics

and to calculate a premium based on that group's level of risk. Those with similar risk pay the same premiums. The process of risk classification provides the fundamental framework for the current private insurance system in the United States. It is essential to insurers' ability to determine premiums which are: (1) adequate to pay their customers' future claims; and (2) fair relative to the risk posed by proposed insureds.

The price of life, disability income and long term care insurance is generally based on the proposed insured's gender, age, present and past state of health, possibly his or her job or hobby, and the type and amount of coverage sought. Much of this information is provided directly by the proposed insured.

Depending on the proposed insured's age, medical history, and the amount of insurance applied for, the insurer may also need information from the individual's medical records. In this event, when the insurer's sales representative takes the consumer's application for insurance, he will request that the applicant sign an authorization, provided by the insurer, authorizing the insurance company to: (1) obtain his health information from his doctor or from a hospital where he has been treated; and (2) use that information to, among other things, underwrite that individual's application for coverage. Based on this information, the insurer groups insureds into pools so that they can share the financial risk presented by dying prematurely, becoming disabled, or needing long term care.

If a company is unable to gather accurate information or have access to information already known to the proposed insured, an individual with a serious health condition, with a greater than average risk, could knowingly purchase a policy for standard premium rates. This is known as "adverse selection." While a few cases of adverse selection might not have a significant negative impact on the life, disability income, or long term care insurance markets, multiple cases industry-wide would likely have such an effect. This would be particularly true if individuals were to be legally permitted to withhold or restrict access to medical information significant to their likelihood of dying prematurely, becoming disabled or requiring long term care. The major negative consequence of adverse selection would be to drive up costs for future customers which could price many American families out of the life, disability income, and long term care insurance markets.

Most life and long term care insurance and much disability income insurance is individually underwritten. As part of the underwriting process, insurers selling life, disability income, and long term care insurance rely on an applicant's individually identifiable health information to determine the risk that he or she represents. Therefore, medical information is a key and essential component in the process of risk classification.

Once a life, disability income, or long term care insurer has an individual's health information, the insurer controls and limits who sees it. At the same time, insurers must use and disclose individually identifiable health information to perform legitimate, core insurance business functions.

Insurers that sell life, disability income, and long term care insurance must use individually identifiable health information to perform essential functions associated with an insurance contract. These basic functions include, in addition to underwriting, key activities such as claims evaluation and policy administration. In addition, insurers must also use individually identifiable health information to perform important business functions not necessarily directly related to a particular insurance contract, but essential to the administration or servicing of insurance policies generally, such as, for example, development and maintenance of computer systems.

Also, life, disability income, and long term care insurers must disclose individually identifiable health information in order to comply with various regulatory/legal mandates and in furtherance of certain public policy goals such as the detection and deterrence of fraud. Activities in connection with ordinary proposed and consummated business transactions, such as reinsurance treaties and mergers and acquisitions, also necessitate insurers' use and disclosure of such information. Life, disability income, and long term care insurers must disclose individually identifiable health to: (1) state insurance departments in connection with general regulatory oversight of insurers (including regular market conduct and financial examinations of insurers); (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), concerned with insurers' market conduct; and (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations. Limitations on these disclosures would operate counter to the consumer protection purpose of these disclosure requirements.

Life, disability income, and long term care insurers need to (and, in fact, in some states are required to) disclose individually identifiable health information in order to protect against or to prevent actual or potential fraud. Such disclosures are made

to law enforcement agencies, state insurance departments, the Medical Information Bureau (MIB), or outside attorneys or investigators who work for the insurer. Again, any limitation on an insurer's ability to make these disclosures would undermine the public policy goal of reducing fraud, the costs of which are ultimately borne by consumers.

III. SUMMARY OF ACLI COMMENTS ON THE PROPOSED RULE

A. Comments Concerning Life and Disability Income Insurers

The impact of the proposed rule on insurers selling life insurance and on insurers selling disability income insurance would be significant and adverse. The proposed rule generally encourages and, in many cases, requires limitation on disclosure of individually identifiable health information. As discussed above, such information is essential to the business of insurance. We are concerned that in an effort to protect confidentiality, the rule will jeopardize insurers' ability to issue, administer and service life and disability income insurance policies.

It appears that the Department does not intend disability income insurance policies to be health plans under the rule. We strongly believe that this is appropriate. However, the proposed rule is not clear on this point. We urge the Department to amend the rule to specify that disability income insurance policies are not health plans.

Section 164.508 requires either an authorization requested by the individual or by a covered entity. The authorization forms submitted by life and disability income insurers to covered entities on behalf of or as authorized by applicants apparently fall within the scope of Section 164.508(a), authorizations requested by individuals. Given the critical importance of protected health information to life and disability income insurers' ability to serve their customers, we believe that this section requires clarification. Section 164.508(a)(1) should provide for the release of protected health information requested by the individual or *authorized by the individual.*

Subject to limited exceptions, the proposed rule requires that a covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the purpose of the use or disclosure. If Section 164.508(a)(1) is not amended to accommodate authorizations submitted as authorized by the individual, covered entities—third parties such as doctors and hospitals—will be charged with determining how much protected health information is the "minimum necessary" for an insurer to underwrite or pay a claim. This result would appear to be contrary to the Department's intent as set forth in the preamble. It would also be inappropriate because it is the insurer, not the covered entity, which will bear the financial risk of the insurance transaction.

We are very much concerned by the standard articulated in Section 164.506(c)(i) giving individuals the right to enter into agreements with health care provider covered entities to restrict the use or disclosure of specified health information. Although this subsection clearly provides that "a covered entity that is a health care provider must permit individuals to request that uses or disclosures of protected health information for treatment, payment, or health care operations be restricted" (emphasis added), the reference to this standard in Section 164.506(c)(2) does not similarly make it clear that: (1) only health care provider covered entities are subject to this standard; and (2) the right to restrict only extends to use or disclosure of protected health information for treatment, payment, or health care operations. We are gravely concerned that if Section164.506(c)(2) is not clarified, it may be read to permit agreements to restrict disclosure of information which could cause material information to be withheld from an insurer underwriting an application or evaluating a claim under a life or disability income insurance policy, without the insurer even knowing that information existed at all. This could result in serious adverse selection, jeopardizing the current private systems of life and disability income insurance. It would legalize actions which constitute fraud and material misrepresentation under current law.

We suggest more reasonable treatment of psychotherapy notes and research information unrelated to treatment. We believe that all individually identifiable health information should be treated confidentially and in the same manner. We are concerned by discussion in the preamble that seems to sanction segregation of psychotherapy notes. We are concerned by the definition of psychotherapy notes as currently proposed which may bar legitimate access to anything more than "summaries of" diagnosis, functional status, etc.

The level of specificity required in the authorization form and the requirement of multiple authorizations are impracticable. Furthermore, we are concerned that giving individuals an opportunity to revoke their authorization for disclosure of protected health information could jeopardize life and disability income insurers' ability

to investigate material misrepresentation, fraud, and claims. We have provided the Department with specific recommendations for amendments to these sections.

B. Comments Concerning Long Term Care Insurance

We believe strongly that long term insurance policies are inappropriately characterized as health plans, making long term care insurers covered entities. We believe that long term care insurance policies should be stricken from the list of coverages defined as health plans. Whether or not long term care insurance policies are health plans, we have the same concerns, as we have with respect to life and disability income insurers, about the proposed rule's impact on long term care insurers' ability to obtain from other covered entities protected health information essential to underwrite and pay claims.

We believe Section 164.508(a) should be amended to clarify that authorizations may be submitted on behalf of or *authorized by an individual.* If Section 164.508(a) is not amended in this manner, covered entities inappropriately will be charged with determining the minimum amount of protected information necessary for long term care insurers to underwrite applications for long term care insurance coverage and to pay claims.

We are particularly concerned about the impact on long term care insurers of the right to restrict use and disclosure of certain protected health information granted under Section 164.506(c)(1). This provision could have a devastating effect on long term care insurers by virtue of the fact that it would permit an agreement to restrict disclosure of information material to "payment" of a long term care insurance claim without a long term care insurer even knowing any information is being withheld. Moreover, the failure of Sections 164.506(c)(2) and 164.512(d)(ii)(B) to clarify that the right to restrict use and disclosure of protected health information is only applicable to treatment, payment, and health care operations could result in interpretation of these subsections to permit agreements to withhold information material to the underwriting of long term care insurance policies. On a widespread basis, this could jeopardize the process of risk classification in relation to long term care insurance.

The special treatment of psychotherapy notes and research information unrelated to treatment, as well as the definition of psychotherapy notes also give rise to concern as they relate to long term care insurance. Again, we believe that all individually identifiable health information should be treated confidentially and in the same manner. We are concerned by discussion in the preamble that seems to sanction segregation of psychotherapy notes. We are concerned by the definition of psychotherapy notes as currently proposed which may bar legitimate access to anything more than "summaries of" diagnosis, functional status, etc.

The requirements for authorizations are particularly troublesome as applied to long term care insurer covered entities. This is especially true with respect to the right to revoke. Given the fact that the definitions of health care operations and payment fail to include a number of essential ordinary insurance business functions of long term care insurers, individuals are given the right to revoke long term care insurers' right to use protected health information for some activities which are critical to the issuance, servicing and administration of long term care insurance policies. The level of specificity required in the authorizations is also problematic as applied to long term care insurers.

If long term care insurers continue to be covered entities in the final rule, we suggest a number of amendments to accommodate the administrative needs of long term care insurer covered entities, just as an apparent attempt was made to accommodate the administrative needs of other covered entities. If long term care insurers are to be covered entities, they should not be treated as "second class" covered entities.

As mentioned above, we are very concerned that the proposed definitions of health care operations and payment do not adequately address key activities of long term care insurers necessary for support of payment. As a result, Section 164.506(a)(1)(i) does not permit long term care insurers to use and disclose protected health information without authorization to perform functions which are "compatible with and directly related to . . . payment" of claims submitted under long term care insurance policies. This would seem to be counter to the stated intent of the proposed rule" to make the exchange of protected health information relatively easy for health care purposes."

We oppose the extension of the proposed rule to business partners of covered entity long term care insurers. We are particularly concerned that long term care insurers are made liable for violations of the proposed rule by their business partners. We are also opposed to the creation of a private right of action by making subjects

of protected health information third party beneficiaries of contracts between long term care insurers and their business partners.

We have a number of important technical concerns with the provisions in Section 164.510 providing for disclosures without an individual's authorization. We include suggestions as to how these matters can be resolved.

While the ACLI supports providing individuals rights of notice, access, accounting for disclosures, and the opportunity to request amendment/correction of inaccurate information, we are very concerned by the burdensome nature of several of these requirements. For example, required and permissible disclosures must be distinguished in the proposed notice. This is in addition to a separate requirement that the notice contain a description of the types of disclosures that may occur. Moreover, the authorization section contains similar disclosure requirements. We suggest several ways in which these overlapping requirements can be simplified without compromising the goal of providing consumers with meaningful information about how a covered entity handles and protects the consumer's protected health information.

The ACLI looks forward to working with the Chairman and members of this committee as Congress addresses the critical issue of protecting the confidentiality of health information.

Confidentiality of Medical Information

Principles of Support

Life, disability income, and long-term care insurers have a long history of dealing with highly sensitive personal information, including medical information, in a professional and appropriate manner. The life insurance industry is proud of its record of protecting the confidentiality of this information. The industry believes that individuals have a legitimate interest in the proper collection and use of individually identifiable medical information about them and that insurers must continue to handle such medical information in a confidential manner. The industry supports the following principles:

1. Medical information to be collected from third parties for underwriting life, disability income and long-term care insurance coverages should be collected only with the authorization of the individual.
2. In general, any redisclosure of medical information to third parties should only be made with the authorization of the individual.
3. Any redisclosure of medical information made without the individual's authorization should only be made in limited circumstances, such as when required by law.
4. Medical information will not be shared for marketing purposes.
5. Under no circumstances will an insurance company share an individual's medical information with a financial company, such as a bank, in determining eligibility for a loan or other credit—even if the insurance company and the financial company are commonly owned.
6. Upon request, individuals should be entitled to learn of any redisclosures of medical information pertaining to them which may have been made to third parties.
7. All permissible redisclosures should contain only such medical information as was authorized by the individual to be disclosed or which was otherwise permitted or required by law to be disclosed. Similarly, the recipient of the medical information should generally be prohibited from making further redisclosures without the authorization of the individual.
8. Upon request, individuals should be entitled to have access and correction rights regarding medical information collected about them from third parties in connection with any application they make for life, disability income or long-term care insurance coverage.
9. Individuals should be entitled to receive, upon request, a notice which describes the insurer's medical information confidentiality practices.
10. Insurance companies providing life, disability income and long-term care coverages should document their medical information confidentiality policies and adopt internal operating procedures to restrict access to medical information to only those who are aware of these internal policies and who have a legitimate business reason to have access to such information.
11. If an insurer improperly discloses medical information about an individual, it could be subject to a civil action for actual damages in a court of law.
12. State legislation seeking to implement these principles should be uniform. Any federal legislation to implement the foregoing principles should preempt all other state requirements.

AMERICAN FEDERATION OF STATE,
COUNTY AND MUNICIPAL EMPLOYEES, AFL–CIO
WASHINGTON, DC 20036–5687
February 16, 2000

The Honorable William Thomas
Ways and Means Committee
Health Subcommittee
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Thomas:

The American Federation of State, County and Municipal Employees (AFSCME) appreciates the opportunity to submit a statement for the record for the February 17, 2000 hearing on the confidentiality of patient records. AFSCME represents over 1.3 million workers. Among these are 360,000 health care workers including registered and licensed nurses, pharmacists, physicians and nursing assistants. Therefore, we approach privacy regulations from the perspective of consumers of health care services as well as workers in the health care system.

We commend the Department of Health and Human Services for addressing the crucial issue of medical record confidentiality in such a comprehensive proposal. The need to develop regulations that will serve as standard protections for the users of health care services is urgently needed in the rapidly changing world of health care delivery.

AFSCME strongly supports the approach in the Health Insurance Portability Accountability Act (HIPAA) and the Department's proposal that federal regulations will serve as a floor, rather than a ceiling, on privacy protections afforded by states. Under this approach, a minimum federal standard would extend important protections to all consumers, but state laws providing greater protections would remain in place or could be enacted in the future to meet new needs.

While the regulations create important new protections, there are areas where the Department stopped short of fully exercising its authority under HIPAA or did not provide adequate clarification in the regulations. We are submitting comments to the Secretary which detail these issues. Many of these issues are summarized below.

The regulations should apply to both electronic and non-electronic health information. Consistent treatment of health information provides a much more workable framework for covered entities. Otherwise, covered entities would need to keep track of the method of transmittal of information from all paper records in order to determine which information in an individual's file is protected. Further, because most information is not maintained in electronic form, the failure to cover paper records provides a gaping hole through which much confidential information can be transmitted despite Congress' desire to protect the privacy of an individual's health records.

The regulations must clarify that protected health information obtained by an employer sponsored self-funded or insured plan cannot be shared with other parts of the employer's organization. If it is not made clear that private health information cannot be shared, it will be used improperly by some employers to make such employment decisions as promotions, job assignments and firings.

The regulations must extend privacy protections to medical records connected to workers' compensation claims. There is a serious problem of unlimited access to and misuse by employers and insurers of individually identifiable health information of workers who have filed such claims. Medical records have been used to discriminate, harass, blacklist and deny workers their rights under the law. We do not believe that Congress intended to exempt workers' compensation insurers from the scope of coverage and believe that the Department should address this subject.

Thank you for the opportunity to submit a statement for the record for this important hearing.

Sincerely,

CHARLES M. LOVELESS
Director of Legislation

CML:bcc
cc: Rep. Pete Stark, Ranking Member

Statement of American Healthways, Inc., Nashville, TN

American Healthways, Inc. ("AMHC"), the successor corporate name of American Healthcorp, Inc., appreciates the opportunity to submit the following comments for inclusion in the record of the House Ways and Means Health Subcommittee Hearing on Patient Record Confidentiality on February 17, 2000.

Overall AMHC strongly supports the proposed privacy regulations published at 64 Fed. Reg. 59,918 (Nov. 3, 1998), particularly the inclusion of disease management in the definition of treatment. It is imperative to legitimate disease management organizations that **the use and disclosure of identifiable health information for disease management be permitted without individual authorizations.** This is currently permitted in the proposed regulations and is essential to the continued operation and success of disease management programs. AMHC and similar disease management organizations, however, are extremely concerned about the lack of a uniform standard. Accordingly, AMHC believes that **complete federal preemption of all state medical privacy laws is imperative**

AMHC, headquartered in Nashville, Tennessee, is the nation's leading operator of care and disease management services with 160,000 lives under management. AMHC's Diabetes Healthways[SM], Cardiac Healthways[SM], and Respiratory HealthwaysSM programs have proved effective at significantly improving health status and decreasing overall cost for these disease populations.

The privacy of individually identifiable health information is of utmost importance to AMHC. AMHC has extensive policies and procedures to protect patient confidentiality. As a result, neither AMHC nor its clients have received a single confidentiality or privacy complaint regarding AMHC's disease management programs. AMHC provides these comments to the Subcommittee from this perspective.

DISEASE MANAGEMENT IN THE PROPOSED REGULATIONS

The proposed regulations allow a covered entity to use or disclose protected health information without individual authorization "to carry out treatment, payment, or health care operations."[1] "Treatment" is defined as "the provision of health care by, or the coordination of health care (including health care management of the individual through risk assessment, case management, and *disease management*) among, health care providers; the referral of a patient from one provider to another; or *the coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual*."[2] Under this definition, use and disclosure of protected health information for disease management is permissible without individual authorization.

It is imperative that this be maintained. The use of identifiable health information without patient authorization is essential to the ability of disease managers such as AMHC to provide and obtain the greatest benefits for patients from its disease management services.

AMHC has utilized both an enrollment or "opt-in" model and an engagement or "opt-out" model for its disease management programs. Under the enrollment model, individuals choose whether to participate in the disease management program. In an engagement model, plan members are automatically provided the benefit of the disease management program, but may choose to "opt-out" of participation. Although an argument might be made that the enrollment model provides greater privacy protection, it unnecessarily intrudes upon the existing coordination of care, producing vastly inferior health care outcomes to the engagement or "opt-out" model.

By way of direct comparison, AMHC documented that with the engagement model AMHC's programs achieve *98 percent* participation, compared to *less than 30 percent* for a typical enrollment model. Additionally, cost savings are dramatically less for an enrollment model. For example, annualized diabetes health care cost savings for an average 100,000 member plan under the engagement model is $1,738,716 as compared to only $443,550 for an enrollment model.

The reason for the difference in participation rates and cost savings is that people with chronic diseases often suffer from inertia and denial about their disease. The engagement process circumvents this avoidance tendency. Typically, the individuals who opt-in are the healthier patients who are already highly motivated to manage their disease. These people are less in need of the extensive disease management

[1] 64 Fed. Reg. 59,918, 60,053 (Nov. 3, 1998).
[2] *Id*. (emphasis added).

programs and, therefore, the clinical improvements in these patients (with their concomitant cost savings), while still present, are less significant.

An engagement model strikes the right balance between the competing interests of individual privacy rights on the one hand and the tremendous clinical and financial benefits of disease management on the other. Allowing individuals to opt-out still provides individuals a choice and yet retains the tremendous clinical and financial benefits of disease management for the largest number of individuals. Moreover, because disease managers are business partners, confidentiality of protected health information remains protected from secondary use or disclosure. Accordingly, disease management programs must be allowed to continue to use and receive protected health information for disease management without patient authorization.

COMPLETE FEDERAL PREEMPTION

In the proposed regulations, HHS states "HIPAA provides that the rule promulgated by [HHS] may not preempt state laws that are in conflict with the regulatory requirements and that provide greater privacy protections."[3] Although HHS may lack the authority to preempt state privacy laws, complete preemption of state laws is imperative. AMHC thus far has managed to operate in compliance with all applicable state laws. However, maneuvering around the varying and often incompatible requirements of so many state laws has been difficult. Soon, the task may be impossible. Since the nation's attention has been focused on medical records privacy issues, many states have enacted new privacy laws and almost all states have significant privacy legislation pending.

California recently enacted a new privacy statute which only allows disclosure of identifiable health information for disease management if the services are approved by the patient's primary care provider.[4] The health plans, more often than providers, contract with AMHC for the provision of disease management services. Individuals, therefore, are entitled to disease management services by virtue of their membership in the plan, not as a function of their relationship with a physician. Individuals should be able to decide whether to "opt-out" of participation in the disease management program offered. Physicians should not be permitted to impede the provision of these services to their patients. The requirement that the physician authorize disease management services imposes an additional administrative burden that will substantially diminish the number of Californians who may benefit from disease management services.

Some state privacy laws directly conflict with others, making it impossible to provide the same, consistent services to residents of different states. Health plans that contract with national employers (*e.g.*, Federal Express) want and need to provide a uniform set of benefits to all their employees. This is impossible with the varying and often conflicting state laws and requirements. In addition, a health plan which is national in scope (*e.g.*, Cigna) needs the ability to sell and deliver uniform products, again extremely onerous, if not impossible, without one uniform standard.

Furthermore, disease managers such as AMHC must keep abreast of all state laws and ensure compliance with each state's nuances, requirements and prohibitions. This is becoming extremely difficult and significantly adds to the cost and burdens on the delivery of health care, generally, and disease management services, specifically.

Finally, it is often difficult to know which state's laws apply. It is conceivable that for one transfer of protected health information, several states' laws could be applicable. For example, in the disclosure of protected health information from a health plan to a disease management organization, the following state laws could apply: (1) the state in which the health plan (the disclosing entity) is based, (2) the state in which the business partner (the receiving entity) is based, (3) the state in which the health care services contained in the protected health information were rendered, (4) the state in which the disease management services are provided and (5) the state in which the individual patient resides. Thus, it is entirely possible that inconsistent standards and requirements could apply to one disclosure or use of protected health information. The uncertainty of which laws apply as well as the complexity and difficulty in complying with the various state laws will likely cripple the delivery of health care and disease management services, especially as states continue to enact more sophisticated, complicated and extensive health care privacy legislation.

Accordingly, to preserve the continued provision of high quality, affordable health care including disease management services, complete federal preemption of state privacy laws is imperative. Without preemption, the processes associated with the

---

[3] *Id*. at 59,926.

[4] *See* Cal. Civil Code § 56.10(17) (West 1999).

delivery of health care could come to a screeching halt as they did in Maine when that State enacted an over-zealous privacy law.[5]

Congress should either provide HHS with such preemption authority or themselves exercise congressional authority to provide complete federal preemption of state medical privacy laws. One consistent, uniform standard, especially given the electronic world in which we now find ourselves, is absolutely imperative and urgently needed. Congress has the authority to preempt state laws in this area as the electronic exchange of identifiable health information involves interstate commerce as it is an interstate activity. Health plans, employers, providers and disease managers often provide services to individuals in multiple states. Accordingly, Congress must exercise its preemption authority to ensure uniformity and clarity in the use, disclosure and protection of identifiable health information.

ABOUT AMHC

AMHC uses identifiable health information provided by its contractors—typically health insurance companies—in its Diabetes Healthways℠, Cardiac Healthways℠ and Respiratory Healthways℠ programs to identify individuals with the targeted disease, determine what level of intervention is required, and monitor, coordinate, and integrate the care of those individuals. Release of identifiable health information to AMHC without individual authorization is essential to the continued operation of AMHC's disease management programs. If authorizations were required before each use or disclosure, disease management programs would be impeded, if not halted, and their tremendous clinical and financial benefits diminished.[6]

AMHC's population management programs are comprehensive health management systems driven by proactive interventions to identify, manage and coordinate the care of populations affected by cardiac or respiratory disease or diabetes. AMHC works with physicians, inpatient caretakers and other medical professionals to develop the best possible care plans for patients. AMHC's services are in the direct chain of care, providing extensive patient services, including health risk assessment, education, care plan development and management, concurrent care review, one-on-one self-care counseling, and primary care physician support and education.

Population-based disease management programs produce significant clinical improvements and financial savings. AMHC's programs are a primary example. A peer-reviewed study of Diabetes Healthways' Diabetes NetCare℠ program concluded that the program "generated substantial gross cost savings" and resulted in "substantial improvement in all of the clinical measures collected."[7] Specifically, "[m]embers were more likely to receive HbA1c tests, foot exams, eye exams, and cholesterol screenings while enrolled in the program . . . [and h]ospital utilization decreased dramatically for each plan's diabetic population."[8] Hemoglobin A1c testing, a signal measure of health status among people with diabetes, increased *127 percent* during the first year of the program. Cardiac Healthways℠ also produces impressive clinical improvements. The ACE inhibitor, cholesterol testing, and beta blocker compliance, the benchmark cardiac care protocols, improved *23 percent*, *61 percent*, and *62 percent*, respectively, during year one for AMHC's cardiac populations.

AMHC's programs also produce significant financial benefits. The Diabetes Healthways℠ program resulted in a *12.3 percent* gross financial savings during the first year, and increased savings each year thereafter. "Hospital costs decreased by $47 per diabetic plan member per month, or $564 per year."[9] Patients in the Cardiac Healthways℠ program achieve even more dramatic first-year savings, an average of *62 percent* for patients suffering from congestive heart failure. These savings also increase year after year as a result of AMHC's aggressive preventative measures for less severely ill patients that delay or prevent the otherwise inevitable onset of complications associated with diabetes and cardiac disease. Other disease management programs have achieved noticeable results as well.

AMHC contracts with and provides disease management services on behalf of health plans and obtains identifiable health information directly from the plans. AMHC runs the information through an AMHC developed algorithm to determine which individuals likely have diabetes, cardiac or respiratory disease and what level of intervention is required. AMHC attempts to extract *all* individuals with diabetes,

---

[5] The law was swiftly repealed.

[6] *See* Robert J. Rubin et al., Clinical and Economic Impact of Implementing a Comprehensive Diabetes Management Program in Managed Care, 83 J. Clin. Endocrinol. and Metab. 2635, 2640 (1998) for a discussion of the benefits of disease management.

[7] *Id*. at 2640.

[8] *Id*. at 2640–41.

[9] *Id*. at 2641.

coronary or respiratory disease. AMHC's population management approach is unique in that it manages the health care of the entire population with certain chronic conditions, regardless of the severity of the illness, historical cost, co-morbid complications or preexisting conditions.

The algorithm does result in some false positives. To ensure that an individual is not falsely identified as having diabetes or cardiac disease, AMHC contacts the individual's physician to verify the diagnosis. Any false positives are removed from the population and some unidentified individuals, missed by the algorithm, are added. If the false positives are not caught through this method, individuals still have the opportunity to opt-out of the program if they do not have the targeted disease (or for any reason). In addition, under the proposed regulations, individuals are always afforded the opportunity to amend any incorrect health information in their records. Regardless, AMHC never discloses identifiable health information other than to its employees or agents implementing the disease management program or to individuals' physicians.

Once AMHC has the targeted disease population extracted, identified individuals are sent a letter, on health plan letterhead, describing the program. Individuals have the opportunity to opt-out of participation. As discussed more fully, infra, Diabetes Healthways[SM] has used both an engagement (opt-out) and enrollment (opt-in) model of participation. The engagement model achieves a *98 percent* participation rate while an enrollment model results in *less than 30 percent* participation.

Once an individual is part of the disease management program, AMHC assumes responsibility for *all* the health care of affected populations, whether or not related to the named chronic disease, and coordinates the care wherever it is delivered: at home, in the hospital, in the physician's office, or in any other outpatient or inpatient setting. Both Diabetes Healthways[SM] and Cardiac Healthways[SM] do, and Respiratory Healthways[SM] will, provide disease management for all individuals in the targeted disease population and monitor and coordinate all their health care in all health care settings. These comprehensive programs have achieved great success.

Overall, AMHC strongly supports the proposed privacy regulations as drafted. AMHC appreciates the Department of Health and Human Services' ("HHS") recognition of the importance of legitimate disease management through its inclusion in the definition of treatment. Disease management programs such as AMHC's Diabetes Healthways[SM], Cardiac Healthways[SM] and Respiratory HealthwaysSM produce tremendous clinical benefits to the patient public (not to mention concomitant financial savings) and, therefore, should be encouraged, not hindered by the privacy regulations.

Statement of American Psychoanalytic Association, New York, NY

The Health Information Privacy Regulations proposed by the Administration on November 3, 1999 represent one of the most thoughtful efforts to date to address the growing threat to the privacy of identifiable health information. The preamble to the regulations sets forth the most thorough analysis of the importance of medical information privacy to quality health care and the public's confidence in the health delivery system. With the exception of the protection for "psychotherapy notes," however, the privacy protections in the proposed regulations do not fulfill the promise of the preamble.

As the preamble notes, the preservation of health information privacy is a "major concern" of citizens. Health information privacy is also essential for quality health care because without an assurance of privacy, individuals will not make the disclosures to physicians and other caregivers necessary for treatment and diagnosis, caregivers will not accurately record information in the medical record and individuals will refrain from seeking the care they need.

The preamble correctly notes that an assurance of "strict confidentiality" is essential for patients to receive effective psychotherapy. That conclusion is supported by the "reason and experience" reflected in the therapist-patient privilege which is recognized by the statutory laws in all 50 states and the District of Columbia, both federal and state common law, the ethical standards of every mental health professional association, and the recently released Surgeon General's Report on Mental Health. The common thread of all of these laws and standards is that therapist-patient communications cannot be disclosed beyond the therapist without the patient's consent.

The underlying statute directs the Secretary to issue regulations that address at least the rights that individuals "should have" with respect to their identifiable health information. The preamble notes that privacy is a fundamental right which

is an element of the constitutional right to liberty, but the regulations make no mention of an individual's right to privacy for identifiable health information.

The regulations also eliminate the traditional requirement of obtaining patient consent before disclosing identifiable health information except for marketing and certain other "non-health" related uses. Accordingly, these regulations would permit disclosure of most identifiable health information for most uses without patient notice or consent.

In an exception to the general rule, the regulations require consent for the disclosure of "psychotherapy notes" for the purposes of treatment, payment and health care operations. The regulations, however, permit the disclosure of psychotherapy communications that do not come within the narrow definition of "psychotherapy notes" and do not recognize even that narrow exception for 13 other uses characterized as "national priorities." Accordingly, the regulations do not afford the protection for psychotherapy communications that is generally accepted as being essential for effective psychotherapy services.

The preamble to the regulations recognizes that statutory authority has not been granted to permit effective enforcement of the privacy protections contained in the regulations. Further, the protections in the regulations are unenforceable because, in the absence of notice of specific disclosures or consent, individuals will have no way of knowing when, where and to whom their information was disclosed. Two of the principal privacy protections in the regulations—the limitation on disclosures to the minimum information necessary for the intended use and the "right to restrict" disclosures that are otherwise allowable—are particularly unenforceable. The information necessary for an intended use varies with the size and technical capability of the disclosing entity, and providers have a right to refuse any request to restrict disclosures.

The regulations appropriately do not preempt state privacy laws, including state common laws, which furnish "more stringent" privacy protections. The recognition of state common laws is particularly appropriate because most privacy protections are found in state common laws, and those court rulings reflect the history of "reason and experience" in those states.

The American Psychoanalytic Association believes that the following changes must be made in the regulations if the public's confidence in the health delivery system is to be preserved:

1. Individuals' right to privacy for identifiable health information should be expressly recognized.
2. The right of patients to give or withhold consent for most disclosures should be preserved.
3. The regulations should establish "strict confidentiality" protections for mental health information and specify the information that may be disclosed with patient consent to third party payors. This approach is consistent with federal and state common law and has been in effect for 15–20 years in New Jersey and the District of Columbia.
4. The privilege recognized for psychotherapist-patient communications in the 1996 Supreme Court decision in Jaffee v. Redmond should be recognized in the regulations. They also should provide that any disclosure for a purpose under the regulations will not constitute a waiver of the federal or state privilege.
5. Patients should be permitted to preserve the privacy of their health information by paying for services with their own funds.

Privacy is essential for quality health care, but it is also an indispensable element of the right to liberty—one of the core principles of our Constitution. These principles have been forged and preserved through the sacrifices of prior generations. With the consideration of the right to medical privacy, we reach one of those critical points in our nation's history when we must decide whether we remain committed to those principles.

Statement of William C. McGinly, Ph.D., CAE, President, Association for Healthcare Philanthropy, Falls Church, VA

The Association for Healthcare Philanthropy (AHP) is pleased to present its comments for the written record on the proposed rules concerning the standards for privacy of individually identifiable health information. (At your request, please be advised that our comments also are submitted on an IBM compatible 3.5-inch diskette in MS Word format.)

Summary and Introduction

Established in 1967, the Association for Healthcare Philanthropy (AHP) is a not-for-profit organization whose 2,850 members manage philanthropic programs in 1,700 of the nation's 3,400 not-for-profit health care providers. As AHP's president and chief executive officer, I can tell you that an estimated 75% to 80% of the U.S. population resides in the areas served by these providers, which include community hospitals and medical centers (59%), multihospital systems (14%), specialty institutions (8%), academic institutions (5%), long-term care facilities (5%), and other not-for-profit facilities (9%).

AHP's members raised more than $5.7 billion in FY1998–$1.92 billion more than was raised by all of United Way of America during the same time period.

Funds raised by AHP's members directly support health care programs and services that are unfunded or underfunded by other sources. These include:

- programs to promote healthy behaviors;
- a vast array of community wellness programs, from mobile health vans to mammography screenings and hearing and eye exams; and
- much needed facility improvements and essential equipment upgrades.

Such programs are central to the not-for-profit mission of AHP members' institutions and organizations. They are an integral part of their business. For such programs to continue, AHP's members must have access to their health care provider's database. The reason: More than 60% of funds raised each year come from individuals-most of whom are grateful patients.

In approaching prospective patient donors, AHP members are sworn to respect the confidentiality of patient information through the AHP Statement of Professional Standards and Conduct and its companion Bill of Donor Rights. Further, AHP members are committed to upholding the spirit and intent of state and federal laws governing use of patient information. The way in which AHP members' institutions and organizations handle confidential information might be likened to how colleges handle student records. That is, academic records are not released without authorization, even to tuition-paying parents, yet demographic data routinely is given to the alumni office for fund-raising efforts that ensure the support of the college's long-range educational mission.

AHP respectfully requests that the proposed regulations be amended so that they neither block nor reduce our members' ability to raise funds for not-for-profit public health care programs.

More specific comments and related amendatory language follow.

Background: Need for Privacy Standards

AHP fully supports the development of standards that protect the confidentiality of individually identifiable health information. However, those standards should be moderated so that they also protect the public health care benefits generated by philanthropic gifts to not-for-profit providers.

This balance of private need and public good is the essence of an underlying tenet of a democratic society, and it is one that AHP believes should be written into these regulations.

Statutory Background

AHP contends that the regulations as proposed would not meet the statutory requirements for the privacy standards, which require that any privacy standard adopted to implement the Health Insurance Portability and Accountability Act of 1996 (HIPAA) "shall be consistent with the objective of reducing the administrative costs of providing and paying for health care [emphasis added]."

By restricting AHP members' access to patient databases, the proposed regulations threaten to destroy a major funding source for public health care, that is, grateful patients. More than 60% of all philanthropic gifts to not-for-profit health care providers come from individuals, most of whom are grateful patients. If access to grateful patients had been restricted in FY1998, when AHP members raised more than $5.7 billion for public health care programs, those programs might have lost as much as $3.42 billion.

Thus, the proposed regulations include a substantial hidden cost.

Consultations

AHP appreciates the opportunity to increase awareness of health care philanthropy and its role in paying for health care, and to propose alternate language in a number of sections in the proposed regulations.

Summary and Purpose of the Proposed Rule

AHP supports the Secretary's recommendation for comprehensive rules that would, among other goals, "(a)llow for the smooth flow of identifiable health information for treatment, payment, and related operations, and for specified additional purposes related to health care that are in the public interest [emphasis added]."

AHP proposes that the final regulations can only meet this goal if they specify that not-for-profit health care providers' fund-raising programs are operated in the public's interest as an integral part of the providers' business operations; therefore, these programs should be included in the smooth flow of identifiable health information.

Specifically, in Paragraph 5, AHP would have the fund-raising

activities of not-for-profit health care providers included under "health care operations" that do not require individual authorization.

Applicability

AHP endorses the applicability of the privacy standards to the entities that include the health care providers that employ AHP members, but again urges the Secretary to make philanthropy programs a permissible use of individually identifiable health information, without authorization, as part of a provider's "health care operations."

Definitions

Health information: AHP generally supports the definition of "health information" and the applicability of the privacy standards to health information. However, a minimum amount of health information is often helpful to the professional development officer-if only to exclude certain constituent groups from messages likely to be deemed offensive. For instance, the following tenets usually guide AHP members when they handle sensitive health information:

- "Donor acquisition" mailings that go to former patients or their families simply do not refer to patients' recent hospitalizations or their illnesses.
- In cases where a patient has freely shared personal information regarding medical conditions, or has expressed an interest or made previous donations to a specified program or department, segmented appeals for related medical causes may occur, but these, too, do not expressly refer to patients' illnesses.
- Patients hospitalized or treated for psychiatric and substance abuse treatment are routinely omitted from donor acquisition approaches because of the heightened sensitivity commonly associated with these diagnostic groups. Also excluded are all minors.
- In general, philanthropy programs give careful thought to the audience and message of all fund-raising appeals, and where appropriate eliminate any constituent groups and/or messages deemed likely to be offensive to recipients.

T3Business partner: AHP supports the definition of "business partner," but would like to establish an understanding about how the definition relates to the ways that health care philanthropy programs are structured.

- Nearly 70% of AHP members work not for the health care provider but for separately incorporated foundations, which are recognized as charitable entities under 501(c)(3) of the federal tax code. It is imperative that the proposed privacy standards not inadvertently close the door to charitable gifts that support public health programs-and provide donors with a valued income tax deduction.
- About 25% of AHP members work for stand-alone departments within the health care provider institution.
- The other 5% work in offices with some other structure. Whether the privacy standards apply to these various structures as "covered entities" or "business partners," it is critical that the standards not limit the effectiveness of health care philanthropy programs to raise money from the people most likely to give, that is, grateful patients.

Individually identifiable health information: A minimum of patient demographic information is essential so that health care philanthropy programs can carry out their not-for-profit mission. Age is needed to exclude minors from appeals.

Introduction to General Rules

The health care philanthropy programs managed by AHP members would not appear in conflict with this broadly stated intent, if "health care" is broadly construed to include public health.

Use and Disclosure for Treatment, Payment, and Health Care Operations

AHP supports the uses and disclosures permitted without authorization in this section, but adamantly opposes the exclusion of certain activities from the definition of "health care operations." The very ability of not-for-profit health care providers

to fulfill their altruistic mission is threatened by the proposed requirement that advance authorization is necessary for the following activities:

- marketing of health . . . services;
- marketing by a non-health related division of the same corporation; and
- fund raising.

With buy-outs by for-profit health care providers threatening the existence of not-for-profits, marketing is critical to the future viability of these altruistic providers. Much of what is marketed by AHP members-from departments or divisions within a provider's corporation or from its related foundation (see "definitions" above)-has tremendous benefit for community health. Wellness programs, mammography screening, ear and eye exams, etc., are marketed by AHP members. Many of these programs are funded by the philanthropic programs that AHP members manage.

One only need look at the hospital wings donated by grateful patients, or the donor recognition plaques that line hospital corridors, to realize that patients are grateful for hospital services and do not mind showing their appreciation with tangible gifts. AHP contends that these gifts are willingly made because they are asked for after services have been received. To ask for them in advance-which would be the effect of the proposed privacy standards-would easily alienate the largest prospect pool for philanthropic gifts to not-for-profit health care providers.

Finally, the kind of marketing carried out by AHP members is not the kind of marketing of commercial products that seems to be the real target of this regulation's restriction. It is important that the final version of the privacy standards distinguish between for-profit and not-for-profit ventures.

In short, AHP would strike these activities from the list of activities that require prior authorization:

- marketing of health . . . services;
- marketing by a non-health related division of the same corporation; and
- fund raising.

Further, AHP would expressly permit not-for-profit health care providers and their business partners to use and disclose protected information without authorization for the following activities that are central to their altruistic mission:

- marketing programs that promote the health of the community; and
- raising funds that support charitable, educational, or research purposes and capital improvements.

Minimum Necessary Use and Disclosure

AHP members already adhere to the practice of minimal use and disclosure. On becoming members, they pledge to uphold the AHP Statement of Professional Standards and Conduct, which requires that an individual's right to privacy be respected and that information gained in the pursuit of professional duties remain confidential. A copy of the AHP Standards is enclosed.

To manage effective philanthropic programs, AHP members minimally need the names of patients and relatives, their addresses and telephone numbers, and their age (to eliminate minors). A minimum of health information is helpful (to eliminate patients with sensitive diagnoses).

Right to Restrict Uses and Disclosures

AHP members already restrict use and disclosure of information gained in pursuit of their professional duties, as part of the AHP Statement of Professional Standards and Conduct (copy enclosed).

Creation of De-Identified Information

AHP supports the use of protected health information for statistical and analytical reports. In fact, AHP annually conducts its Survey on Giving, through which members share information about health care philanthropy. AHP is the only source of this data in the country, which each year is given to the American Association for Fund Raising Counsel for its comprehensive report, Giving USA.

Application to Business Partners

The philanthropy efforts of AHP members are structured in several ways-as foundations, as stand-alone departments or divisions, or in other ways. However efforts are structured, whether they are construed as "covered entities" or "business partners," it is paramount that these regulations permit access to protected data without authorization.

Application to Information About Deceased Persons

AHP supports this regulation's intent to be sensitive to the families of the deceased. However, AHP respectfully suggests that providing its members with protected information is more likely to achieve this goal than the converse. After all, AHP members cannot exclude families of the deceased from general appeals for philanthropic gifts if the fact of death is not known.

Furthermore, when friends or family of the deceased wish to make a memorial gift, AHP members must have the minimum demographic information to accommodate this wish.

Adherence to the Notice of Information Practices

AHP supports the intent of this section, which requires that information uses and disclosures reflect the actual notice of such use and disclosure. Again, however, AHP urges that the philanthropic programs managed by its members be included under "health operations" that do not require advance authorization for what is a central component of the mission and business of not-for-profit providers.

Uses and Disclosures with Individual Authorization

This section contains one phrase that reveals the intent of its authors: commercial gain. AHP could not agree more that individuals have the right to refuse the release of protected information that will result in commercial gain to the requesting entity. No commercial gain is possible for not-for-profit health care providers, and privacy standards must distinguish between for-profit and not-for-profit entities.

The philanthropic programs of AHP members should be considered an integral part of the provider's "health operations" and thus be exempt from individual authorization. That is the current practice, and AHP can attest to the fact that its members hear only rare concerns which are quickly resolved after they explain the health services, research, and educational programs that are supported by philanthropy.

Aside from the inappropriateness of applying this standard to not-for-profit health care providers, the proposed authorization form is onerous and counterproductive. Picture a patient in serious condition, being admitted to a hospital, being handed all the usual forms and one asking for permission to solicit contributions at a later date. A hospital with a form like this would be showing very little sensitivity to the patient and would likely receive no gift at a later date, even if the patient were grateful for the medical treatment received.

Introduction to Rights of Individuals

AHP supports the rights of individuals as delineated in the proposed regulations and assures the Secretary that its members swear to respect those rights through the AHP Statement of Professional Standards and Conduct.

Rights and Procedures for a Written Notice of Information Practices

AHP believes that the health services, research, and educational programs supported by the philanthropy programs of not-for-profit health care providers are an integral part of "health operations" and should be treated as such in this and other sections of the final regulations.

Rights and Procedures for Access for Inspection and Copying

AHP believes that the health services, research, and educational programs supported by the philanthropy programs of not-for-profit health care providers are an integral part of "health operations" and should be treated as such in this and other sections of the final regulations.

All of AHP's comments are offered with the sincere appeal that the new regulations should be structured so as to take into account the professional ethical standards already in place. These regulations must allow for the continued work of hospitals and health-related foundations in philanthropic programs that benefit individuals and communities . . . benefits which, if lost, would be severely detrimental to the quality of life. AHP looks forward to working with the Department in order to preserve the charitable fund-raising activities of not-for-profit health providers while respecting an individual's appropriately limited individually identifiable health information.

We appreciate the opportunity to comment on the proposed standards. More importantly, we look forward to actively assisting the Department in developing protective patient medical record regulations while safeguarding our non-profit providers' obligation to meet their charitable purposes and fully serve their patients.

Professional Standards and Conduct from Association for Healthcare Philanthropy

Association for Healthcare Philanthropy members represent to the public, by personal example and conduct, both their employer and their profession. They have, therefore, a duty to faithfully adhere to the highest standards and conduct in:

I. Their promotion of the merits of their institutions and of excellence in health care generally, providing community leadership in cooperation with health, educational, cultural, and other organizations;

II. Their words and actions, embodying respect for truth, honesty, fairness, free inquiry, and the opinions of others, treating all with equality and dignity;

III. Their respect for all individuals without regard to race, color, sex, creed, ethnic or national identity, handicap, or age;

IV. Their commitment to strive to increase professional and personal skills for improved service to their donors and institutions, to encourage and actively participate in career development for themselves and others whose roles include support for resource development functions, and to share freely their knowledge and experience with others as appropriate;

V. Their continuing effort and energy to pursue new ideas and modifications to improve conditions for, and benefits to, donors and their institution;

VI. Their avoidance of activities that might damage the reputation of any donor, their institution, any other resource development professional or the profession as a whole, or themselves, and to give full credit for the ideas, words, or images originated by others;

VII. Their respect for the rights of privacy of others and the confidentiality of information gained in the pursuit of their professional duties;

VIII. Their acceptance of a compensation method freely agreed upon and based on their institution's usual and customary compensation guidelines which have been established and approved for general institutional use while always remembering that: any compensation agreement should fully reflect the standards of professional conduct; and, antitrust laws in the United States prohibit limitation on compensation methods;

IX. Their respect for the law and professional ethics as a standard of personal conduct, with full adherence to the policies and procedures of their institution;

X. Their pledge to adhere to this Statement of Professional Standards and Conduct, and to encourage others to join them in observance of its guidelines.

A Donor Bill of Rights

Philanthropy is based on voluntary action for the common good. It is a tradition of giving and sharing that is primary to the quality of life. To assure that philanthropy merits the respect and trust of the general public, and that donors and prospective donors can have full confidence in the not-for-profit organizations and causes they are asked to support, we declare that all donors have these rights:

I. To be informed of the organization's mission, of the way the organization intends to use donated resources, and of its capacity to use donations effectively for their intended purposes.

II. To be informed of the identify of those serving on the organization's governing board, and to expect the board to exercise prudent judgment in its stewardship responsibilities.

III. To have access to the organization's most recent financial statements.

IV. To be assured their gifts will be used for the purposes for which they were given.

V. To receive appropriate acknowledgment and recognition.

VI. To be assured that information about their donations is handled with respect and with confidentiality to the extent provided by law.

VII. To expect that all relationships with individuals representing organizations of interest to the donor will be professional in nature.

VIII. To be informed whether those seeking donations are volunteers, employees of the organization or hired solicitors.

IX. To have the opportunity for their names to be deleted from mailing lists that an organization may intend to share.

X. To feel free to ask questions when making a donation and to receive prompt, truthful and forthright answers.

Developed by American Association of Fund Raising Counsel (AAFRC) Association for Healthcare Philanthropy (AHP) Council for Advancement and Support of Education (CASE) National Society of Fund Raising Executives (NSFRE). Endorsed by (in formation) Independent Sector National Catholic Development Conference (NCDC) National Committee on Planned Giving (NCPG) National Council for Resource Development (NCRD) United Way of America

Statement of Association of American Medical Colleges

The Association of American Medical Colleges (AAMC) is pleased to submit its views on the Department of Health and Human Services Notice of Proposed Rulemaking (NPRM) "Standards for Privacy of Individually Identifiable Health Information." The AAMC represents this nation's 125 accredited medical schools, approximately 400 major teaching hospitals and health care systems, and 91 academic and professional societies representing over 75,000 faculty members. Our members and institutions provide basic and specialized healthcare services, conduct research leading to the discovery of medical knowledge and the development of innovative treatments and therapies, and educate and prepare physicians to meet evolving health care needs. Whether in utilizing health information in treating patients, educating future physicians, or conducting clinical research ranging from the etiopathogenesis of disease, translation and clinical trials to studies in epidemiology, prevention and health services, the AAMC is keenly aware of the need to protect the privacy of individuals and the confidentiality of individually identifiable health information.

The AAMC strongly believes that the only comprehensive and nationally coherent solution to the complex and emotionally charged problems of "medical information privacy" lies in federal legislation, and we have steadfastly supported the enactment of such to strengthen the protection of individuals' personally identifiable health information from inappropriate disclosure and harmful misuse. Any legislation will require a balancing between protecting individuals' health information and allowing health care entities and providers reasonable access to information that can be shared for purposes of treatment, research, and education.

The NPRM's preamble articulates the department's concern with its limited authority under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the rationale for the stratagems it devised to craft regulations with the broadest possible reach in the face of those limitations, and it is punctuated with repeated calls for federal legislation as the much preferred approach. These points are important to understanding the structure, complexity and potential impact of the regulations that have been proposed. The preamble seeks frequent refuge in the principles articulated in Secretary Shalala's thoughtful report to the Congress in September 1997, entitled "Confidentiality of Individually Identifiable Health Information." At the time, the AAMC expressed its strong general support of the principles, while noting their ultimate acceptability would turn on the details of their implementation, which the report did not address. Given the complexity of the proposed regulations, their substantial financial and administrative costs, and the profound operational and behavioral changes that they would impose at every level of the health care delivery system, it is ironic to note that the relevant HIPAA authority derives from the Administrative Simplification provisions of the Act (Sections 261–264).

Although the AAMC appreciates the work the department has invested in this NRPM, we have very serious reservations about certain of the approaches and implementation steps. We fear that they would impose unreasonable burdens and unwise constraints on the day-to-day functioning of the health care delivery system and the conduct of medical research. While fully supporting the individual's right to privacy and respecting the need for effective, systemic protections of the confidentiality of individually identifiable health information, we believe that some of the standards, implementation requirements, and procedures imposed by this NPRM would have real costs that far outweigh their theoretical benefits. We believe that the NPRM requires major changes so that it will reasonably protect the privacy of individually identifiable health information without impeding the flows of health information required for the care of patients, the operations of the health care delivery system, or the conduct of health research. In particular, the AAMC draws attention to the following salient concerns:

- **Impact on Delivery of Health Care:** The enactment and implementation of any standards for medical information privacy will impose enormous costs and administrative burdens on the U.S. health care system. In this regard, any federal regulations must be crafted with precision and with understanding of and sensitivity to the complexity and magnitude of the flows of individually identifiable health information involved in the health care of patients. Unfortunately, the AAMC finds that many of the proposed provisions in the NPRM impose unreasonable burdens and unwise constraints on the day to day functioning of the health care delivery system. In particular, the AAMC believes the concepts and applications of "business partners," "minimum necessary," and "de-identified protected health information"

are poorly devised and ill-conceived. In addition, the language establishing a "code of fair information practices" with respect to individual access, amendment, and correction of protected health information (PHI) needs to be more carefully tailored to the realities of the complex patterns and enormous volumes of continuous health information traffic that are necessary for the health care delivery system to function. We urge the department to reconsider the proposed regulations in the NPRM, which would unjustifiably and unnecessarily impede the critical functions of the day-to-day operations of the entire U.S. health care system.

- **Intrusion on Research:** The AAMC strongly opposes the approach taken in the NPRM to divide medical research information into two broad classes, one "related," the other "unrelated," to treatment. HIPAA gives the HHS no authority to regulate researchers. However, the NPRM attempts to do so by regulating covered health care providers who are also researchers. The AAMC finds this approach unnecessary and poorly conceived. The distinction of research information categories as described by the NPRM, in fact, would serve to weaken the protections of confidentiality of research data that are currently available, while imposing heavy burdens on medical researchers, and would be of little or no benefit to the safeguarding of individually identifiable health information. Rather than separating research information that is "related or unrelated to treatment," the AAMC believes that information obtained from research that is clinically relevant to the care of the subject should be entered into the individual's medical record. Thereby, the formal "research record" would remain separate from the medical record. It is the Association's strong position that research information and clinical information can and should be maintained separately, primarily to afford the research information a much higher degree of security than can be afforded to clinical information and medical records.

- **Impact on Common Rule:** The attempt by the department to regulate issues related to "protected health information" (PHI) in research is problematic. In the NPRM's preamble, the department notes that HIPAA gives HHS no authority to regulate health researchers. Research involving human subjects is already subject to the Common Rule. However, the NPRM attempts to amend the Common Rule by adding four new criteria to those already required of IRBs in consideration of waiver of individual authorization. The AAMC strongly opposes this effort at piecemeal modification of the Common Rule. The Association is unaware of any credible evidence indicating that protection of the confidentiality of PHI used in research is not being adequately respected and protected by IRBs and researchers working under the requirements of the existing Common Rule. Moreover, with the imminent relocation and reorganization of the OPRR in the Office of the Secretary and formation of a new National Advisory Council for the new Office, the scrutiny of human research subjects protections underway by the NBAC, and similar studies being conducted by the IOM, the department's approach is particularly untimely. The AAMC strongly urges the department to abandon this ill-advised approach and continue to regulate all research and researchers identically under the provisions of the Common Rule.

- **Preemption of State Law:** The AAMC strongly believes, and has consistently argued, that the workings of the contemporary health care delivery system, the mobility of American citizens, and the needs of medical research, especially population-based research, all call for federal legislation that would strongly preempt state law (with only few limited exceptions for such things as public health reporting) and establish a single, uniform national standard of medical information privacy protection. The department does not favor such "strong" preemption, and in any event asserts correctly that it does not have authority under HIPAA to impose it by regulation. The NPRM would establish a federal floor of protections and would preempt only contrary provisions of state laws that are less stringent than those imposed by the regulation. It would thereby permit what is often described as a patchwork of discordant state privacy laws of variable effectiveness to remain in place. The NPRM's lengthy disquisition on the interpretations of "contrary to," "less stringent" and "more stringent" underscores the confusion and significant burdens that the lack of a single, preemptive federal standard will place on covered entities whose professional activities and business transactions increasingly span state lines. The entities would have to comply not only with the federal rule but with the more stringent provisions of state law in every state in which they operated. The AAMC is deeply concerned about the chaotic business climate and extraordinary legal expenses that would result from the imposition of this regulation, and fears that as it is proposed, it will be unworkable. The AAMC would urge the Secretary to conduct a state-by-state examination and certify those state laws that she deems "contary and more stringent than" the federal rules. All other state laws bearing

on medical information privacy would thereby be deemed to be preempted by the new rule.

Although the AAMC appreciates the effort that the HHS has invested in developing this proposal, the AAMC feels that many of the standards in the NPRM would not in actual practice serve to enhance protections of the privacy and confidentiality of individuals proportionately to the burdens and complications that they would impose on critical functions of the affected entities. In several instances, the department has exceeded the authority granted to it under HIPAA, a fact that underscores the need for Congress to revisit this complex issue to ensure that a system of protection of individually identifiable health information is logical, coherent and nationally uniform, not needlessly burdensome and costly, and will neither impede health care delivery nor vital health research. While fully supporting the individual's right to privacy and respecting the need for effective, systemic protections of the confidentiality of individually identifiable health information, the implementation of the standards and procedures imposed by this NPRM would have real costs that far outweigh their theoretical benefits and would serve to deter legitimate and useful sharing of information that may be vital for treatment, research and medical education.

Statement of Jane M. Orient, M.D., Association of American Physicians and Surgeons, Inc., Tucson, AZ

The Association of American Physicians and Surgeons (AAPS), founded in 1943 to protect private medicine and the patient-physician relationship, represents physicians in all specialties nationwide.

Both Congress and the White House have expressed well-founded concerns about the privacy of medical records. However, proposed legislation, as well as the standards on "the privacy of individually identifiable health information" recently promulgated by the Department of Health and Human Services as mandated by the Health Insurance Portability and Accountability Act, would have an effect opposite to the stated intention of protecting patient confidentiality. Both the proposed regulations and various legislative proposals establish procedures permitting and facilitating the disclosure of information for which disclosure is now either prohibited or practically impossible.

The objective of writing standards for the electronic transmission of data has been subverted into a pretext for changing the fundamental ethics of the patient-physician relationship and the purpose of medical records.

In the tradition of Hippocrates, the physician serves the patient, who trusts him to abide by the precept that "All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and never reveal." The traditional medical record consists of the physicians' notes and other data, such as laboratory reports, related to the specific, narrow purpose of providing optimal care to the individual patient. The actual information in the record belongs to the patient, who traditionally has had control over the dissemination of that information.

The proposed regulations overturn these basic principles. The patient's right to refuse consent to release his records is abrogated. All patients (or at least those who have any medical records in electronic format) are thus required to serve administratively determined societal objectives: "health services research" as well as medical research; the detection and prosecution of violations of any law, rule, or regulation; monitoring physician compliance with practice "guidelines—and central allocation of resources. All of these are generally irrelevant to and may actually be contrary to the best interests of the patient. "National priorities," undefined or vaguely defined, are held, at the discretion of an administrative agency, to override the individual's right to liberty (as the liberty to seek care from a physician who guards patients' privacy). Individual Fourth Amendment rights are easily swept aside by assertion of a collective "need." Vastly expanded administrative powers trump the requirement for judicial procedure to obtain a search warrant.

While medical professionals will be placed in the dilemma of violating their professional ethics or committing a federal crime by not releasing data, they will also be held responsible, under pain of prison and enormous fines, for monitoring behavior of other entities with which they contract but over which they have little control. Additionally, they will be required to implement costly and onerous notification and other paperwork requirements that actually provide no meaningful patient protection.

In short, proposed rules and laws serve the interest of expanded use rather than real protections. The expanded use may serve some narrow special interests as well

as regulators and prosecutors but will be of very questionable medical or scientific value, especially since accuracy will be compromised by the withholding of sensitive information.

We recommend the following:

1. A moratorium on the proposed regulations. (Comments submitted to HHS are appended.)

2. Legislation that embodies the following basic principles:

a. The right of all Americans to seek medical treatment outside of any medical insurance plan in which they may be enrolled should be explicitly guaranteed especially (but not exclusively) if the plan requires electronic data storage or transmission as a condition of coverage.

2. Electronic data storage or transmission should require the patient's explicit, fully informed consent before the data are entered.

3. No medical professional may be required to perform any act that violates his conscience as a condition of being permitted to practice his profession or specialty.

4. Patients should have a cause of civil action against any individual, including an agent of the government, who causes him harm by the misuse of computerized data. To this end, any electronic data processing system established under this Act should include a mechanism for tracking all individuals who access identifiable records.

CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES
February 14, 2000

The Honorable Donna E. Shalala
Secretary of Health and Human Services
200 Independence Ave. SW
Washington, D.C. 20201

Dear Secretary Shalala:

We are writing to comment on the proposed rule on standards for privacy of individually identifiable health information that was published in the Federal Register on November 3, 1999.

We commend you for moving forward swiftly with this effort and for the thorough and thoughtful discussion contained in the proposed rule. Because Congress did not meet its self-imposed August 21, 1999, deadline for passing medical privacy legislation, the proposed rule is an important and necessary step toward addressing the pressing need for health information privacy protections.

We believe that the proposed rule as a whole provides a solid foundation of privacy protections that will improve our health care system. It establishes strong privacy requirements while ensuring access to health information for important public interest purposes such as health research. However, several significant gaps in privacy protection remain. Some gaps relate to statutory constraints on your authority to regulate, including the lack of privacy restrictions applicable to entities that receive individually identifiable health information but are not covered by the rule and the lack of a private right of action that would enable individuals to seek redress for privacy violations. Other gaps include the exclusion from coverage of certain entities that provide insurance coverage for health care services, and the lack of sufficient restrictions on law enforcement access to individuals' health information.

Congress should work to pass legislation that builds on the proposed rule and addresses issues the proposed rule does not cover. We have sponsored comprehensive medical privacy legislation that we believe would accomplish these goals. We hope to continue to work with you and other interested parties to promote the passage of meaningful medical privacy legislation. In the meantime, we urge you to issue final medical privacy regulations expeditiously, so that the public's medical records are protected as soon as possible.

The following are our comments on specific aspects of the proposed rule.

I. SCOPE

We agree with the approach discussed in the proposed rule's "Applicability" section to apply privacy protections to individually identifiable health information that has been transmitted or maintained electronically regardless of whether the information remains in electronic form. One of the goals of Congress in enacting the 1996 Health Insurance Portability and Accountability Act (HIPAA) was to provide

for the establishment of an effective privacy protection system for health information. A privacy protection policy that would deny access to health information when it is on a computer, but allow access once the information is printed off the computer onto paper or discussed orally by those viewing the computer screen would leave gaping holes in protection. To ensure a meaningful system of privacy protection that is consistent with congressional intent, it is appropriate and necessary to protect health information that has been transmitted or maintained in electronic form even where the information does not remain in electronic form.

Nevertheless, we are concerned that the protections set forth in the proposed rule do not apply to health information that has *never* been maintained or transmitted electronically. We agree with your analysis that a primary concern of HIPAA was that computerization of the health care system was increasing apprehension about electronic dissemination of health information. Any comprehensive medical privacy protection system, however, should ensure that individuals' identifiable health information in any form will receive appropriate privacy protections. It should not be legal to sell an individual's health record for marketing purposes just because the record happens to have been maintained only in paper form. We have reviewed your analysis concluding that you have authority to apply your proposed rule to records maintained solely in paper form and agree that you do have such authority. We urge you to exercise your full authority and apply the proposed rule to records maintained solely in paper form.

With respect to the scope of entities covered by the proposed rule, we are concerned that, in the "Definitions" section, the proposed rule excludes certain insurance entities such as auto insurers from the definition of "health plan" (referencing 29 U.S.C. 1186(c), which has been renumbered 29 U.S.C. 1191b(c)). Under the proposed rule, an auto insurer that pays health care costs associated with an individual's broken arm would not be subject to federal privacy restrictions regarding the health records used in the payment transaction. At the same time, a health plan that pays for treating the broken arm *would* be subject to federal privacy restrictions regarding the records used in the payment transaction. It does not make sense to make such a distinction among insurers who are paying for health care, and we do not believe that HIPAA mandates this distinction between insurers with respect to medical privacy regulations. We urge you not to exclude the types of insurance coverage listed in 29 U.S.C. 1191b(c) from the rule when such coverage pays the cost of medical care.

Further, any comprehensive medical privacy law should apply privacy protection requirements to all entities that obtain protected health information. As you know, because statutory constraints limited the proposed rule's applicability only to health plans, health care providers, and health care clearinghouses, the proposed rule does not reach a number of entities that obtain individuals' health information. This means that, under the proposed rule, a health researcher could obtain health information from a health care provider for health research, and then disclose it to marketers or the individual's employer with no restrictions. We will continue to press for the passage of legislation which applies privacy protection requirements to all appropriate entities.

II. GENERAL RULES

The proposed rule's sections entitled "Introduction to General Rules" and "Minimum Necessary" set forth basic rules that are essential to medical privacy protection. Any comprehensive medical privacy law should prohibit the use or disclosure of individually identifiable health information without the individual's authorization or specific authorization by law. Medical privacy law should also ensure that, where use or disclosure of such information is authorized, entities take all reasonable steps to use non-identifiable (or de-identified) health information instead of identifiable health information. Further, medical privacy law should require that identifiable information will be used and disclosed only to the minimum extent necessary to accomplish the legitimate purpose for which it was obtained. These ground rules establish clear presumptions that use and disclosure of individually identifiable health information will be limited and narrowly tailored to legitimate purposes. We are pleased that the proposed rule includes provisions that reflect these principles.

III. CONTENT OF AUTHORIZATION FORM

The proposed rule's section entitled "Individual Authorization" establishes necessary requirements for the content of authorization forms. Authorization forms should contain sufficient information to ensure that individuals can make informed authorization decisions. We are concerned that individuals seeking health treatment are vulnerable to requests from health care providers and others to authorize uses and disclosures of their health information for purposes beyond treatment, payment,

and health care operations. Individuals in such a situation should have a clear understanding that their treatment and payment are not conditioned on providing authorizations to allow their health information to be used for marketing, by their employers, or for other purposes. Individuals also should be informed to the maximum extent practicable about how their information would be used and disclosed under the authorization.

It would be insufficient, for example, to seek an authorization from an individual but to only describe to the individual generally what uses and disclosures are legal. Rather, individuals should be informed of the purposes for which the information is sought as well as the proposed uses and disclosures of the information. In addition, the authorization form itself should state that treatment and payment are not conditioned on agreeing to the authorization. The proposed rule includes such content requirements, and therefore we believe that the authorization content required by the proposed rule will facilitate informed consent.

IV. INDIVIDUAL RIGHTS

The proposed rule provides individuals with rights that are integral to ensuring that they have appropriate information about and involvement with their own health records. In the sections entitled "Access for Inspection or Copying" and "Amendment or Correction," the proposed rule providesimportant rights that enable individuals to access, copy, and correct their own records, so that individuals can have a remedy when inaccurate information in their records is being used in transactions that affect them. Further, the requirements in the "Accounting of Disclosures" and "Notice of Information Practices" sections that covered entities must provide individuals with a notice of their information practices and the opportunity to review accounting of certain disclosures are necessary to ensure that individuals have appropriate information about the uses and disclosures that occur regarding their own health records.

We request, however, that you review your decision not to include a requirement that covered entities obtain a signed acknowledgment from individuals stating that the individuals have received the notice and been informed of their rights. Such a requirement, which is included in H.R. 1941, legislation introduced by Mr. Condit, would enhance the right to notice set forth in the proposed rule by encouraging individuals to consider carefully their rights and the information practices that affect them before providing their health information to a covered entity. An alternative approach to encouraging individuals to review and reflect on their medical privacy rights is to require that individuals sign an authorization form before a covered entity may disclose their health information for any purpose. This approach is taken in H.R. 1057, legislation introduced by Mr. Markey.

We recognize the logistical questions you have raised regarding exactly how signed acknowledgments should be provided, and the concerns you discuss regarding requiring authorizations for treatment, payment, and health care operations purposes. We are interested in and look forward to reviewing the comments of relevant parties on these issues. We urge you to continue to work to create optimal conditions for ensuring that individuals engage in meaningful review of their privacy rights and the information practices of covered entities, without imposing inappropriate burdens on covered entities.

With respect to the section entitled "Accounting of Disclosures," we believe that it is important to provide individuals with a means of learning about disclosures that an entity has made of their health information without imposing unnecessarily burdensome accounting requirements on the entity. As you know, the proposed rule attempts to balance these concerns by excluding treatment, payment, and health care operations disclosures from the accounting requirements. The rationale behind the proposed rule's effort to balance these concerns is reasonable. We agree with the proposed rule's analysis that individuals generally have the most interest in disclosures that they cannot easily anticipate will be made with their health information.

However, the definitions of treatment, payment, and health care operations cover a broad range of activities, from determination of coverage, to billing, to utilization review, to disease management, to reviewing the competence of health care professionals, among many other activities. Given this breadth, individuals will not necessarily easily anticipate that their health information will be shared for each type of treatment, payment, and health care operations activity. Therefore, we are concerned that the proposed rule may not provide individuals with adequate means to learn about the disclosures that have been made with their health information. Accordingly, we request that you carefully review whether exclusion of all treatment, payment, and health care operations disclosures from accounting requirements is appropriate.

V. UNDERWRITING

It is our understanding that under current practice, insurers that seek an individual's identifiable health information to conduct underwriting generally first obtain an authorization from the individual that delineates the uses and disclosures that the insurer may make with the information, unless the underwriting activity concerns an existing insurance contract. Several congressional medical privacy proposals, however, contain broad language that would allow insurers to obtain an individual's health information for "underwriting" without obtaining an individual's authorization. We are aware of no good policy reason to encourage in a federal law a change in current practice by allowing underwriting without the patient's permission.

We therefore are pleased that the proposed rule makes clear, in the section entitled "Definitions," that insurers may obtain and use an individual's identifiable health information for underwriting activities without the individual's permission *only*> when the individual is enrolled in the plan conducting the activities and the activities concern an existing contract. We ask that you provide clarification, however, on whether under the proposed rule, authorization from the individual is required for underwriting activity relating to a change in contract within the same health plan, and whether the proposed rule diverges from current practice on this specific issue.

VI. DISCLOSURES FOR HEALTH RESEARCH PURPOSES

Health research is critical to the effective operation of our health care system. Medical privacy law should ensure both access to data necessary for conducting health research and patient confidence in the confidentiality of their health information. Accordingly, we believe that, before individually identifiable health information is disclosed for health research, a board independent from the entities seeking or disclosing individually identifiable health information for health research should review the research and determine that appropriate privacy protections are in place. At the same time, there should be a means of ensuring expedited review where research poses minimal privacy threats. In the section entitled "Research," the proposed rule takes a significant step forward toward accomplishing these goals by including requirements that incorporate elements of the "Common Rule" standards that currently apply to review of federally funded research conducted by institutional review boards (IRBs).

With increased federal restrictions on access to medical records, more and more entities seeking medical records are likely to claim that they are engaged in research. Therefore, review committees internal to such entities would likely face pressures to authorize disclosures that will advance the entity's financial interests. The proposed rule's requirements that no individual on the board reviewing the research can have a conflict of interest with the research and that at least one member of the board cannot be affiliated with the institution conducting the research help address this concern. We believe, however, that the proposed rule would be improved by also including a requirement that the Secretary certify that such boards meet the rule's criteria. This requirement, which is contained in H.R. 1941, establishes a third party mechanism to ensure that board are capable of exercising independent judgment. We urge you to incorporate this requirement into the final rule.

It is worth noting that applying Common Rule standards to review of privately funded research is consistent with the approach advocated in recent testimony before the House Subcommittee on Health and Environment of the Committee on Commerce by both members and chairs of IRBs and representatives of individuals with serious health conditions who have a tremendous personal stake in health research, such as the National Breast Cancer Coalition and the National Organization for Rare Disorders. These witnesses underscored that extending Common Rule protections to all health research not only would be practicable but would benefit health research. For example, Dr. Greg Koski, Director of Human Research Affairs for Partners Health Care System in Boston, who has served over 15 years as a member and chair of an IRB, stated that applying Common Rule protections to privately funded research would improve health research because "by protecting human subjects and by letting them know that we are putting their interests in the appropriate priority, there will be a greater willingness to participate in research." He also noted that additional guidance regarding specific mechanisms for confidentiality protection should be set forth for IRBs.

VII. LAW ENFORCEMENT

The provisions in the proposed rule's section entitled "Law Enforcement" do not establish sufficient privacy assurances to individuals. We believe that, except in emergency circumstances, disclosure of an individual's health records to law enforce-

ment officials should only occur pursuant to a warrant, or if the individual has received notice of the proposed disclosure and has had an opportunity to challenge the disclosure. Such an approach, which is set forth in H.R. 1941, ensures that law enforcement officials do not have unchecked discretion to determine the necessity of obtaining individuals' health records. The proposed rule does not meet this standard, as it allows for disclosure of an individual's personal information to law enforcement officials pursuant to a range of procedures, including a grand jury subpoena, without any neutral third party review or notice to the individual.

VIII. JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

We are concerned that the proposed rule, in the provisions entitled "Judicial and Administrative Proceedings," would allow the disclosure of an individual's health information for a judicial or administrative proceeding simply on the basis of a request from an agency or a counsel representing a party in the proceeding, if the individual's health is at issue in the proceeding. Individuals whose information is the subject of such a request should have notice of the request and an opportunity to challenge the request. We ask that you revise the proposed rule to include this requirement.

IX. ENFORCEMENT

No matter how strong federal privacy protections may be, they will be difficult to enforce unless individuals have the right to seek redress for privacy violations. A private right of action is an essential enforcement tool because the government is not likely to pursue civil sanctions for individual violations. Enforcement through criminal sanctions is also insufficient since prosecutions are brought selectively and face a high standard of proof. Every major privacy bill Congress has enacted, including the Fair Credit Reporting Act, the Cable Communications Policy Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, and the Right to Financial Privacy Act, has contained a private right of action. We understand that you did not have the authority to provide for a private right of action, and we will continue to press to ensure that Congress passes medical privacy legislation that contains this crucial enforcement tool.

X. PREEMPTION

We are pleased that, consistent with the framework set forth in HIPAA, the proposed rule would not preempt state laws that provide greater privacy protections than those in the proposed rule. Setting a federal floor is important because it gives states the ability to enact stronger state privacy laws in those circumstances where they want to address issues of particular concern to their citizens. For example, some states have enacted privacy laws to encourage individuals to get tested or treated for communicable diseases, alcohol and drug abuse, and other conditions. The "floor" approach also allows states the flexibility to protect their citizens regarding specific health crises or concerns that we cannot predict at this time. We will continue to work to ensure that any medical privacy legislation enacted by Congress establishes a federal floor.

We recognize that there may be questions in some instances as to whether an individual state law is more protective than the federal law. H.R. 1941 provides a mechanism for addressing such questions by requiring the Secretary to give advisory opinions as to whether a state law is more protective. We are pleased that, in the section entitled "Relationship to State Laws," the proposed rule provides a similar mechanism by allowing states to request an advisory opinion. We believe, however, that any person, not just states, should be able to seek such an opinion, and urge you to revise the proposed advisory opinion process to allow for such requests.

We strongly believe that state laws that provide greater protections than the proposed rule should not be preempted. We are concerned, however, about the provision in the proposed rule which states that the Secretary may determine that the proposed rule will not preempt a state law if that state law is necessary for "the efficiency and effectiveness of the health care system." Depending on how it is interpreted, this vaguely worded provision could allow a broad range of state laws that are less protective than the proposed rule to stand. We request that you revise this provision to ensure that it does not become a wide loophole for avoiding the proposed rule's requirements.

XI. CESSATION OF OPERATIONS

We are concerned that the proposed rule does not clearly address whether privacy protections would apply to health records maintained by a covered entity once that entity has ceased to do business. We urge you to ensure that health records have appropriate protections in such circumstances, as suggested in H.R. 1941 and as envisioned in H.R. 307, legislation introduced by Mr. Towns.

XII. CONCLUSION

The proposed rule not only establishes a strong foundation of privacy protections, but it presents ideas and arguments that enhance the debate among parties interested in medical privacy policy. We look forward to reviewing the comments of others on the proposed rule and your response to our comments. We will work to ensure that Congress acts to pass legislation that incorporates the important privacy protections included in the proposed rule and addresses areas that require further protection.

Sincerely,

Members of Congress

Gary A. Condit
Henry A. Waxman
Edward J. Markey
John D. Dingell
Sherrod Brown
Edolphus Towns
David E. Bonior
Major R. Owens
Patsy T. Mink
Gene Green
Barney Frank
Lucille Roybal-Allard
Paul E. Kanjorski
Albert Russell Wynn
Fortney Pete Stark
Lynn C. Woolsey
William D. Delahunt
Mike Thompson
John F. Tierney
Carlos A. Romero-Barcelo
Jim McDermott
Janice D. Schakowsky
Neil Abercrombie
Eleanor Holmes Norton
Carolyn B. Maloney
Harold E. Ford, Jr.
John Joseph Moakley
James P. McGovern
Dennis J. Kucinich
Ellen O. Tauscher
Sam Farr
Benard Sanders

cc: U.S. Department of Health and Human Services
Assistant Secretary for Planning and Evaluation
Attention: Privacy-P, Room G–322A
Hubert Humphrey Building
200 Independence Avenue, SW
Washington, DC 20201

February 16, 2000

The Honorable Secretary Donna E. Shalala
Secretary of Health and Human Services
200 Independence Avenue, SW
Washington, D.C. 20201

Dear Secretary Shalala:

We are writing regarding the proposed rule on standards for privacy of individually identifiable health information that was published in the FEDERAL REGISTER on November 3, 1999. We want to associate ourselves with the comments on the proposed rule that were set forth in the February 14, 2000 letter to you from Representatives Gary A. Condit, Henry A. Waxman, Edward J. Markey, John D. Dingell, and 28 other colleagues.

Protecting the privacy of medical records is integral to the effective operation of our health care system. We appreciate your efforts on this important issue and we look forward to continuing to work with you, our colleagues, and others to advance appropriate and comprehensive medical privacy protections.

Sincerely,

Members of Congress

Gerald D. Kleczka
Donna Christian-Christensen
Tom Lantos
Louise Slaughter

cc: U.S. Department of Health and Human Services
Assistant Secretary for Planning and Evaluation
Attention: Privacy-P, Room G–322A
Hubert Humphrey Building

200 Independence Avenue, SW
Washington, DC 20201

Statement of the Consortium for Citizens with Disabilities

I. General Privacy Concerns

The Consortium for Citizens with Disabilities (CCD) is a Washington-based coalition of approximately 100 national disability, consumer, advocacy, provider and professional organizations that advocate on behalf of 54 million children and adults with disabilities and their families in the United States. As advocates for people with disabilities, CCD supports strong privacy protections that give health care consumers confidence that their information will be used appropriately and that permit the continued viability of medical research and delivery of quality health care.

All persons who receive health care services have reason to be concerned with the inappropriate use of highly personal information that is collected about them within the health care system. As a coalition representing people living with disabilities, however, CCD's views on this issue are somewhat unique. Because people with disabilities have extensive medical records and sometimes stigmatizing conditions, such individuals feel a particular urgency to ensure that proper privacy protections are in place. At the same time, many people with disabilities interact almost daily with the medical establishment and thus benefit from a well-run, effective health care system. Such individuals do not want privacy protection to reduce the effectiveness of the health care system they must navigate.

CCD has been actively involved in the medical privacy debate, and believes that the desire for medical privacy and the desire for an effective health care system are neither in conflict with each other, nor do they require "balancing" of one interest against another. Rather, establishing privacy protection can enhance the operation of the health care system, by increasing individuals' trust and confidence in that system. A national survey released in January 1999 found that one in six Americans engages in some form of "privacy protective behavior" because he or she is afraid of confidentiality breaches regarding sensitive medical information. These activities include withholding information from health care providers, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and-in some cases-avoiding care altogether.[1] None of this is good for either consumers or the health care system.

II. General Approach of the Proposed Regulations

CCD applauded the President and the Secretary's action to release the proposed rule. After reviewing the proposal, we continue to believe that the Department of Health and Human Services' efforts hold the potential to significantly increase privacy protections, and equally important, provide people new assurances that their deeply personal medical information will be used appropriately. We also believe that the proposal provides an important foundation for Congress to build upon in protecting privacy and maintaining quality health care. We are particularly pleased that the proposed rule would not pre-empt more protective state laws and acknowledges that people with disabilities and other sensitive conditions may need special protections (such as through the handling of psychotherapy notes). We are also pleased that the proposed rule requires covered entities to contract with business partners and name as third party beneficiaries individuals whose protected health information is used or disclosed. We commend the Secretary for proposing that individuals be permitted to access and copy their health information. We are also pleased that the Secretary acknowledges the continued need for federal legislation to fill gaps the Secretary did not have authority to cover under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

While we acknowledge the leadership of the President and Secretary in moving the process forward, we have found areas in the proposed rule that we find unworkable or that need bolstering.

---

1 California Healthcare Foundation, National Survey: Confidentiality of Medical Records (January 1999). The survey was conducted by Princeton Survey Research Associates. Results are available at www.chcf.org/conference/survey.crfm.

III. The Secretary's Authority Under HIPAA

The delegation under HIPAA limited the Secretary's authority in three important areas. The Secretary only had authority to cover health plans, health clearinghouses and certain health care providers, and information transmitted or maintained electronically. HIPAA also did not provide a private right of action for individuals whose health information has been improperly used or disclosed. We encourage Congress to enact legislation to fill these gaps.

A. Covered Entities

While the Secretary covered entities permitted under HIPAA, unfortunately, many entities (such as life insurers, employers and marketing firms) that receive, use and disclose protected health information are not required to comply with the regulations. We believe that directly covering these entities is necessary to adequately protect patient privacy. While we believe that entities who receive information should be directly covered at the federal level, we commend the Secretary for acting within the limits of HIPAA and constructing the business partner rules to cover entities who regularly use and disclose protected health information.

B. Covered Information

As part of administrative simplification, HIPAA limited the Secretary's authority to protect only information transmitted or maintained electronically. While the Secretary discusses her authority at length, we are concerned that people with disabilities may be reluctant to seek care or to honestly discuss sensitive health conditions if all of their health information is not confidential. Privacy is especially important to people with disabilities because they may have stigmatizing conditions which, if disclosed, could result in discrimination and embarrassment. Because of the complexity of the health care system, most patients will never know what information, if any, is stored electronically. Even if patients are able to determine what information is maintained electronically, they will likely fear that some portion is in paper format. Without privacy protection for all health information, people with disabilities will be reluctant to discuss their condition. We know that this leads to bad health outcomes and, in some cases, would cause people to forego medical care entirely. The only way to ensure patient confidence in the health care system is to make the proposed rule applicable to all information.

C. Private Right of Action

Under the proposed rule, individuals whose protected health information has been improperly used or disclosed will have no recourse. While we recognize that the Secretary did not have authority under HIPAA to create a private right of action, we strongly believe that Congress should enact legislation to fill this important gap. Many federal privacy statutes have private right of action provisions including the Privacy Act of 1974 (5 U.S.C. 552a), Electronic Communications Privacy Act (18 U.S.C. 2701 et seq.), Right to Financial Privacy Act (12 U.S.C. 3401 et seq.), Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), Cable Communications Act (47 U.S.C. 551), Videotape Privacy Protection Act (18 U.S.C. 2710) and the Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.).

IV. Important Areas Where the Regulation Could Be Improved

While we have many concerns with the proposed rule, we believe that the rule provides greater protections than exist today and is an important foundation upon which to build. While we have submitted comprehensive comments to the Secretary, we have highlighted five important areas for people with disabilities, and believe, at a minimum, the following changes are necessary: (1) require covered entities to obtain a written authorization prior to using or disclosing protected health information for treatment, payment and health care operations, (2) require entities to obtain authorization prior to communicating with the individual about sensitive health conditions, (3) require covered entities to first determine whether de-identified information can be used to accomplish the purpose of the use or disclosure, (4) prohibit disclosure of protected health information for law enforcement purposes without a warrant from a neutral judicial officer, and (5) extend protections of the regulations to all individually identifiable health information.

A. Signed Authorization for Treatment, Payment and Health Care Operations

(Section 164.506 Uses and disclosures of protected health information: general rules)

The proposed rule permits covered entities to use and disclose protected health information for treatment, payment and health care operations without individual

authorization. A signed authorization from the individual is extremely important. This issue was addressed at length by the Health Privacy Working Group, a panel comprised of diverse stakeholders including disability and mental health advocates, health plans, providers, employers, standards and accreditation representatives, and experts in public health, medical ethics, information systems and health policy. See Best Principles for Health Privacy, a Report of the Health Privacy Working Group (July 1999). This diverse group noted that, as a general rule, requiring patient authorization prior to disclosure can:

- bolster patient trust in providers and health care organizations by acknowledging the patient's role in health care decisions;
- serve as recognition that notice was given and the patient was aware of the risks and benefits of disclosure; and
- define an "initial moment" in which patients can raise questions about privacy concerns and learn more about options available to them.

We find the Secretary's proposed rule extremely troublesome because it does not require patient authorization, and in fact, prohibits covered entities from obtaining authorizations unless required by State law. Unless the current regulatory authorization for treatment, payment and health care operations is modified, CCD would oppose implementation of this rule. In a world of managed care, the Administration and many health and consumer interests have been dedicated to shifting popular culture to embrace the concept of the "empowered patient." Many observers believe that the best way to make managed care work is for patients to become self-advocates, active in working the system so they get the care they need. Dismantling the current authorization system runs counter to this approach. The Secretary's approach disempowers patients by taking away their ability to actively control access to their own protected health information.

Patients should be encouraged to be active participants in their own health care-and the authorization process should be an integral piece of that picture. A signed authorization provides a unique opportunity for the individual to understand the uses and disclosures of her health information. This process will increase individual awareness of the risks and benefits of such uses and disclosures. While the Secretary states that individuals are not likely to know "all the possible uses, disclosures, and re-disclosures to which their information will be subject," individuals should be informed, to the extent practicable, of how information will be used and to whom it may be disclosed. See 64 Fed. Reg. 59918, 59940 (Nov. 3, 1999). A signed authorization will give individuals an opportunity to review the authorization and create an "initial moment" in which the patient can address her privacy concerns. When discrepancies between an individual's privacy concerns and the covered entity's use and disclosure of information arise, the signed authorization will provide an opportunity for the individual to ask questions about how her information will be used and disclosed.

The Secretary states three reasons for not adopting a signed authorization approach: (1) authorizations provide individuals with little actual control over their health information, (2) consent is often not voluntary because the individual must sign the form as a condition of treatment or payment, and (3) individuals are often asked to sign broad authorizations but are provided little or no information about how their health information will be used. 64 Fed. Reg. 59918, 59940 (1999).

We find the Secretary's rationale troubling. The Secretary has the authority to improve the current authorization process but states current problems as the reason not to empower patients. Even if the Secretary chooses not to empower patients, her rationale that authorizations provide individuals with little actual control and consent is often not voluntary does not consider the importance of the "initial moment." As discussed above, this moment gives individuals the chance to learn about the use and disclosure of her information and ask questions, voice concerns or negotiate, if possible. The Secretary's rationale also fails to consider the reality of receiving medical treatment for sensitive conditions. We know that for stigmatizing conditions, such as HIV or sexually transmitted diseases, individuals exercise control by foregoing treatment or choosing to self-pay for specific services under an assumed name. Authorizations would help these individuals learn more about the use and disclosure of their information so they can feel comfortable receiving treatment and providing accurate information to providers.

Because many covered entities currently obtain signed authorizations, there would be little, if any, additional administrative burden. See 64 Fed. Reg. 59918, 59940 (1999). We see no reason to reduce current protections afforded to consumers. As covered entities increase communications with individuals, provide individuals with opportunities to understand how their information is being used and disclosed, and allow individuals to negotiate, individuals will feel that they have more control

over their health care decisions. These simple but important changes will likely improve the public's perception of the health care system.

B. Individual Authorization for Sensitive Health Conditions

(Section 164.508 Uses and disclosures for which individual authorization is required)

Requiring entities to obtain authorization from an individual before communicating with the individual about sensitive health conditions is also very important. People with disabilities who seek sensitive health care services have heightened concern that their medical condition or treatment may be inadvertently disclosed to others such as roommates, house mates, family members, neighbors, employers or others who may want to cause harm.

Covered entities should be required to protect against inadvertent disclosures of protected health information concerning sensitive health care services [defined as services relating to reproductive health, sexually transmissible diseases (whether or not transmitted in any particular case), substance abuse, or mental health] by obtaining the individual's authorization prior to communicating with the individual (or the policyholder).

Sensitive health care services often involve the most personal health care decisions. Individuals with sensitive health conditions face unique confidentiality concerns because they are the most likely to suffer discrimination or stigmatization associated with such conditions. It is very important that people with disabilities who have sensitive conditions be able to control where and how information about sensitive conditions is communicated to them. For example, a person living with HIV may want to ensure that a covered entity does not send any information about health services to her work address because she fears her employer or co-worker may discriminate against her.

We believe that covered entities should be required to obtain authorization from the individual prior to all communications with the individual regarding sensitive health care services. All communications with the individual should be protected because it is very difficult to determine exactly where in the chain of communication an individual's information could result in stigmatization, discrimination, retaliation or other harm.

The Secretary acknowledged in her prefatory language that covered entities already have the ability to implement and track patient authorizations. 64 Fed. Reg. 59918, 59946 (1999). Furthermore, the regulations require authorizations for (1) uses and disclosures other than treatment, payment and health care operations, (2) uses and disclosures of psychotherapy notes, and (3) uses and disclosures for research unrelated to treatment. Because an authorization framework is in place, we do not believe that an authorization for sensitive health conditions would be a significant burden.

C. De-identified Information

(Section 164.506(b)(1) Standard: minimum necessary)

We strongly believe that entities should first be required to determine whether de-identified information can be used or disclosed to accomplish the intended purpose. While we agree with the Secretary's general approach that entities use or disclose only the minimum amount necessary, we believe that a clear statement that entities must first consider de-identified information is the only way to ensure that the minimum amount standard is adequately implemented.

Requiring entities to use and disclose de-identified information will help ensure that only the minimum amount will be used. Presumably, de-identified information is part of the minimum amount necessary evaluation. While proposed section 164.506(d) defines de-identified protected health information, it is unclear when, if at all, an entity must use de-identified information.

We believe that a de-identified requirement is consistent with the Secretary's proposed minimum amount requirement. In fact, in the prefatory language to the minimum amount requirement, the Secretary notes that stripping individually indentifiable information of identifiers is currently used for analytical, statistical and research purposes. 64 Fed. Reg. 59918, 59946 (1999).

While the Secretary states that section 164.506(d) is intended to permit important research to continue, certainly there are benefits to requiring all covered entities to consider de-identified information. Requiring entities to consider de-identified information will limit the ability of all recipients to link the information to individuals.

D. Law Enforcement

(Section 164.510(f) Disclosures for law enforcement purposes)

We are also very concerned about the Secretary's proposed section 164.510(f). Under the proposed rule, people with disabilities may have their health information

disclosed to law enforcement officials without any legal process. We urge the final regulation require law enforcement to obtain legal process-such as a warrant or court order-that is judicially-approved after application for a Fourth Amendment probable cause standard.

These same requirements exist in other federal privacy statutes protecting peoples' communications, cable subscriber records and even video rental lists. None of these laws are absolute bars to law enforcement access. The procedural safeguards ensure that accountability and oversight prevent unwarranted and unjustified abuse of authority.

E. Paper Records

(Section 164.502 Applicability)

As discussed above, as part of administrative simplification, the Secretary's authority was limited to information electronically maintained or transmitted. We are concerned that people with disabilities may be reluctant to seek care or honestly discuss their health condition if all of their health information is not confidential. Privacy is especially important to those with disabilities because if information about their disability or condition is disclosed they may suffer discrimination, embarrassment or stigmatization. Because of the complexity of the health care system, most patients will never know what information, if any, is stored electronically. Even if patients are able to determine what information is maintained electronically, they will likely fear that some portion is in paper format. Without privacy protection for all health information, persons with disabilities may not disclose their health condition. The only way to ensure patient confidence in the health care system is to make the proposed rule applicable to all information.

IV. Conclusion

We believe that the proposed rule provides an important foundation to protect patient privacy and maintain quality health care. We commend the Secretary for not preempting more protective state laws, acknowledging that sensitive information needs special protection, constructing business partner rules and permitting individuals to inspect and copy their health information. We encourage Congress to enact legislation to build upon these important regulations and to fill gaps left by HIPAA.

Statement of the Family Violence Prevention Fund, San Francisco, CA

I. General Privacy Concerns

The Family Violence Prevention Fund (FVPF) is a leading national organization that advocates on behalf of the millions of women and children who are victims of domestic violence each year. The FVPF runs several major programs that deal specifically with health care and its response to domestic violence, including the national resource center on health care and domestic violence. As advocates for domestic violence victims, the FVPF supports strong privacy protections that will give victims confidence that their personal information will be used appropriately.

Almost onethird of American women report being a victim of domestic violence at some point in their lives. The health care system is playing an increasingly important role in responding to battered women by identifying and documenting abuse and connecting victims with domestic violence advocates and services. Privacy of health information is critical to the safety and wellbeing of millions of women and children who suffer harm from domestic violence and abuse each year. Strong privacy protections that take into consideration the concerns of domestic violence victims will encourage victims to discuss their injuries and feel safe knowing that their information will remain confidential.

A victim is often concerned about privacy because she fears that her perpetrator will discover that she has discussed the abuse with her provider. A perpetrator who learns that his victim has told her provider about the domestic violence could resort to further abuse. Because victims fear that their health information will not remain confidential, many may be reluctant to discuss the violence openly and honestly.

In order to protect victims, many providers do not document domestic violence because they also fear the perpetrator could access the victim's health information and cause additional harm. Providers who discover but do not document domestic violence run the risk that later treating providers will not know the history of violence and misdiagnose the victim. Providers who do not document violence could also reduce the victim's chance of success in legal proceedings against her perpetrator. A complete medical record that fully documents injuries and subsequent health com-

plications from the abuse can be introduced as compelling evidence to corroborate the victim's testimony. Without this corroborative evidence, victims would need to introduce other, less persuasive evidence which could hinder the victim's chance of success. Providers who know that information will remain confidential are more likely to engage the patient, encourage the patient to discuss violence openly and feel comfortable providing a complete record.

For a victim who chooses to be open and honest, privacy concerns only begin when she discusses the violence with her provider. Any communication with the victim at home, including a bill, email or telephone call to confirm an appointment, increases the likelihood that the perpetrator will intercept the information. Individuals who are concerned about their safety should be permitted to give providers a telephone number and address where the victim feels comfortable that the perpetrator will not discover that she has sought treatment.

While the Secretary's proposed regulations are an important foundation and include some measures of protection for victims of domestic violence they fall short of providing the level of privacy safeguards that are necessary to protect victims. We have submitted comprehensive recommendations to the Secretary which we believe are essential for improving the health care, safety and well-being of domestic violence victims. Without these protections, victims of domestic violence will receive inadequate health care services, be less able to pursue effective legal recourse, and potentially be exposed to further violence.

II. The Proposed Regulations

The FVPF believes that the Secretary's proposed regulations have the potential to improve the quality of care for victims of domestic violence by establishing an important foundation that personal medical information will remain confidential. This assurance of confidentiality will likely encourage victims to seek treatment and promote open and honest communication between doctor and patient.

We are particularly pleased that the proposed regulations provide individuals access to their own health information, require notice to patients of confidentiality practices and do not preempt more protective state laws. We commend the Secretary for constructing business partner rules which require covered entities to contract with business partners to whom protected health information is disclosed. We also commend the Secretary for acknowledging the continuing need and importance of comprehensive federal legislation.

III. The Secretary's Authority Under HIPAA

Under HIPAA, the Secretary only had authority to cover health plans, health clearinghouses and certain health providers. The Secretary's authority as part of administrative simplification was also arguably limited to electronically stored or transmitted information and did not include the authority to establish a private right of action. While we believe that the regulations provide an important foundation for privacy protections, we strongly encourage Congress to fill the gaps left by HIPAA.

A. Covered Entities

Acting under the delegation in HIPAA, the Secretary's regulations fall short of covering all entities that receive, use and disclose protected health information. Legislation is needed to protect information received by all entities such as insurance companies, marketing firms and employers. Without covering these entities, victims of domestic violence could be subject to discrimination if an insurance company or employer were to use the information improperly.

B. Covered Information

While administrative simplification under HIPAA arguably limited the Secretary's authority to cover only electronic information, we believe that privacy protections should include all protected health information. By protecting only electronic information, the same concerns about patient confidence that exist today will continue, and many patients will remain reluctant to discuss sensitive health information, even for treatment. Because of the complexity of the health care system, most patients will never know what information if any, is stored electronically. We are especially concerned that many domestic violence victims will continue to hide the real cause of their injuries because they fear for their safety. Even if patients are able to determine what information is maintained electronically, they will likely fear that some portion of the information is in paper format.

C. Enforcement and Private Right of Action

HIPAA only permitted the Secretary to impose civil and criminal penalties for violating privacy standards. In order to provide basic privacy protections afforded to individuals under other federal privacy statutes, Congress should enact legislation that permits individuals to bring a private right of action.

The civil and criminal penalties in HIPAA are not sufficient to ensure that those who inappropriately use or disclose information or fail to adopt adequate safeguards comply with the regulation. We are concerned that Congress has not recognized the need for a private right of action with regard to medical information. Many other federal privacy laws have private right of action provisions such as the Privacy Act of 1974 (5 U.S.C. 552a), Electronic Communications Privacy Act (18 U.S.C. 2701 et seq.), Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), Cable Communications Act (47 U.S.C. 551), Videotape Privacy Protection Act (18 U.S.C. 2710) and the Driver's Privacy Protection Act (18 U.S.C 2721 et seq.). Certainly, highly personal health information deserves the same protections afforded to other information.

IV. Brief Summary of Recommended Changes to the Proposed Rule

Although we have many concerns with the proposed rule, we believe that the rule provides greater protections than exist toady and provides an important foundation upon which to build. While we have submitted comprehensive comments to the Secretary, the following is a brief summary of our recommended changes to the proposed rule.

A. Applicability

We believe that the regulation should apply to health information in both electronic and paper format. By only covering electronic information, the same concerns about patient confidence that exist today will continue, and many patients will remain reluctant to discuss, even for treatment, sensitive health information. Because of the complexity of the health care system, most patients will never know what information, if any, is stored electronically. We are especially concerned that many domestic violence victims will continue to hide the real cause of their injuries because they fear for their safety. Even if patients are able to determine what information is maintained electronically, they will likely fear that some portion of the information is in paper format. The only way to ensure patient confidence in the health care system is to make the proposed rules applicable to all information.

B. Definitions

We agree with the Secretary's proposed rule that a minor who lawfully obtains health care services on his or her own exercises the rights of an individual under the proposed rule. For victims of domestic violence or abuse who are minors, this provision would guarantee that family members who are perpetrators could not access information (see also comments for Directory Information and Next of Kin). We are also concerned about minors who may suffer due to well-meaning but inappropriate parental intervention. For example, a daughter who is abused by her boyfriend may fear that if her parents discover the abuse, they will confront her abusive boyfriend in a cursory or inappropriate manner. As a result, the boyfriend could resort to retaliation and further violence.

C. Treatment, Payment and Health Care Operations

We strongly believe that covered entities should be required to get individual authorization in order to use or disclose protected health information for treatment, payment and health care operations. While the Secretary states that such an authorization is meaningless because individuals must sign the authorization in order to receive treatment, authorizations themselves are very important because they are an "initial moment" in which patients can raise questions about privacy concerns and learn more about options available to them. For many domestic violence victims who are concerned about further violence, this initial moment will help create confidence that their information will be used only for specified purposes.

Providers disclosing information for consultation or referral should be required to verify who is requesting protected health information. We are concerned that victims of domestic violence who receive specialized care (such as reproductive or mental health services) may have their information improperly disclosed to the perpetrator. Under the proposed regulations, a provider who renders specialized services would not be required to consult the patient before disclosing information or even verify who has requested the information. We are concerned that perpetrators could successfully obtain information by using the proposed rule under false pretenses.

The regulations should require a covered entity to protect against inadvertent disclosures of protected health information concerning sensitive health care services

(defined as services relating to reproductive health, sexually transmitted diseases, substance abuse, and mental health) by obtaining an individual's authorization prior to communicating with the individual at the individual's home (whether by phone or mail). Individuals seeking sensitive health care services have a heightened concern that information about their medical condition or treatment may be inadvertently disclosed to others in their household, such as roommates, housemates, or family members. The authorization should specifically ask whether the provider or plan can call the individual at home, send communications via email to the individual's home, or send bills to the individual's home. If the individual does not authorize these communications, the individual should provide on the authorization form a phone number or an address for such communications and must indicate how payment will be arranged if payment is due.

D. Minimum Necessary

We strongly believe that entities should first be required to determine whether de-identified information can be used or disclosed to accomplish the intended purpose. While the proposed rule requires that entities use only the minimum amount of information necessary, the rule does not require the use of de-identified information. We believe that a clear statement that entities must first consider de-identified information is the only way to ensure that the minimum amount necessary standard is adequately implemented.

We also strongly believe that when an entity discloses information at the individual's request, only the minimum amount necessary should be disclosed, unless the individual has indicated otherwise. A victim may authorize a provider to disclose information to a friend or family member in order to discuss her present course of treatment. Under the proposed rule, a provider could disclose the victim's entire medical history including information about domestic violence the victim may have intended to remain confidential.

Where disclosure is not pursuant to a court order, we strongly recommend that only the minimum amount of information necessary to respond to the request be disclosed in judicial and administrative proceedings. While we recognize that litigants may need to access information, we are concerned that covered entities who disclose information would prefer to disclose all information rather than redact sensitive information. Unnecessary disclosure could occur under a number of scenarios, including a subpoena in a personal injury lawsuit where the victim gave a history of prior abuse at the provider's request. While some providers, plans or parties may choose to redact the information, some may not—thereby disclosing sensitive personal information. If the holder of information is unclear what information is being requested, the entity should request clarification and should only disclose that information which is necessary. While the Secretary's preamble raises practical concerns about applying the minimum amount necessary standard requirement in judicial and administrative proceedings, we believe that, at a minimum, only information reasonably necessary to respond to a subpoena should be disclosed (see Judicial and Administrative Proceedings).

We also strongly believe that law enforcement access to protected health information about victims of crime or abuse should be limited to the minimum amount necessary requirement. Providers who disclose too much information to law enforcement without adequate consideration of the victim's safety increases the likelihood that a perpetrator will discover that the victim was treated for her injuries (see Law Enforcement). We are also concerned about victims in small communities who can be easily linked to the information even if the victim's name or address is not disclosed. We believe that the minimum necessary requirement would help prevent these types of inappropriate and unnecessary disclosures.

E. Right to Request Restrictions

An individual should have a true right to restrict the use and disclosure of information that could jeopardize the individual's safety. Women who know that they will suffer further violence from a perpetrator must be able to access health care without fearing such communications will reach him. A victim of domestic violence needs to be able to place restrictions on the use and disclosure of their information even for treatment, payment and health care operations. A victim also needs to know that a perpetrator who requests information will not be able to locate her. It is essential that a victim who has fled a perpetrator not be found because a provider or insurer gave the perpetrator the victim's new address, either directly or through mailing of an explanation of benefits form. A victim's right to restrict the disclosure of her protected health information should not be dependent on an agreement of a health care provider, who may underestimate the severity of danger. Failing to give a victim of abuse a true right to limit disclosures of such information where the dis-

closure would endanger her safety will undermine the efforts of the health care community to serve victims and deprive them of necessary care and assistance.

We also believe that third parties who provide health care services or issue bills independent of the primary provider, insurer, or institution should comply with use and disclosure restrictions requested by an individual. If an individual restricts the use and disclosure of information, a provider who agrees to or is aware of a restriction must inform third parties that the information can only be used and disclosed for purposes that do not violate the restrictions. For example, an individual who is referred to an out-of-plan radiologist may be billed separately for the radiology treatment. So, even if the primary provider's bill goes to an alternate address, the radiologist's bill could be sent to the victim's house, inadvertently notifying the perpetrator and endangering her. If an individual has requested that the original, referring provider only communicate with the individual at an address other than the individual's home, the radiologist should also be required to comply with the restrictions originally requested by the individual. It should always be the primary provider/institution's responsibility to communicate the restriction to all third parties as a patient often does not know which referrals are billed separately.

F. Component Entities

We strongly believe that the Secretary should expressly state that personnel and benefit administration employees responsible for benefits or managing the day-to-day operation of the health plan are covered by the regulation. The Secretary's preamble appears to cover these employees but we believe this should be made clear in the regulation. We also recommend that the Secretary require personnel departments and employees who handle health care administration to have safeguards to ensure that information is not disclosed to the larger organization. We are very concerned about employers who may improperly obtain information from benefit administrators and use the information inappropriately to make employment decisions (such as promotions, job assignments, and even firing). Victims of domestic violence would be likely targets even when they perform well on the job. Employees who work within the health care component must be empowered to deny release of the information to corporate executives and managers outside the health care component unless disclosure is required for health plan administration.

G. Judicial and Administrative Proceedings

We strongly believe that the regulations should specify minimum information that must be included in court and administrative orders in order to guide those disclosing protected health information and to notify those receiving information that the information cannot be used or disclosed for other purposes. At a minimum, court and administrative orders should: (1) provide that the protected health information is subject to court protection; (2) state the nature of the information to be disclosed, and to the extent practicable, identify specific information to be disclosed; (3) specify to whom the information may be disclosed; (4) specify that such information may not otherwise be used or disclosed; and (5) meet any other requirements that the court or tribunal determines are needed to protect confidentiality. These requirements are necessary to ensure that sensitive information is not released outside of the proceedings in a way that could jeopardize the safety of the victim.

We believe that only the minimum amount of information necessary to respond to a subpoena should be disclosed. If the holder of information is unclear what information is being requested, the entity should request clarification and should only disclose that information which is necessary. While the Secretary's preamble raises practical concerns about applying the minimum amount necessary requirement in judicial and administrative proceedings, we believe that, at a minimum, the Secretary should require that only information reasonably necessary to respond to a subpoena should be disclosed. While we recognize that it may sometimes be difficult for parties responding to requests to determine exactly what information the requesting party seeks, the holder of the protected health information should not have blanket authority to disclose all protected health information—only information that is directly responsive to a subpoena should be disclosed. While a victim may have a long history of domestic violence and other conditions, if the information is not directly responsive then it should not be disclosed.

We also strongly believe that the Secretary should include a provision prohibiting disclosure of protected health information unless the individual who is the subject of the information has had (1) reasonable notice of the subpoena and (2) reasonable opportunity to move the court, or other presiding official, to quash the subpoena on the basis that the individual's privacy interest outweighs the interest of the person seeking the information. Under the proposed rule, a domestic violence victim may not know about a request for disclosure of her personal information that could seri-

ously endanger her. A notice requirement would ensure that a victim could take the necessary precautions to make sure that domestic violence information does not reach the perpetrator.

H. Law Enforcement

We are very concerned that domestic violence information may be disclosed to law enforcement officials without any consideration or notice about safety concerns of domestic violence victims. The only way to safeguard the privacy of domestic violence victims is to require a warrant from a neutral judicial officer prior to every law enforcement disclosure. A warrant requirement is a familiar standard in other federal privacy laws and has not been shown to interfere with legitimate law enforcement activity. We are also concerned that without a warrant requirement a victim could be deterred from reporting violence if she knows that the police could access all of her medical records.

A covered entity should be required to provide notice to a victim about any requests or disclosures of information to law enforcement officials. Information released to law enforcement officials will likely be used to make an arrest or conduct follow up investigation. We are concerned that during this process a perpetrator may discover, either directly through police interrogation or indirectly from witnesses who have been contacted, that the victim has discussed the abuse with law enforcement officials or her provider. Providing notice to the victim will allow the victim to take necessary safety precautions. Because providers are already required to account for disclosures we believe that any administrative burden would be insignificant.

When a victim has requested restrictions on uses and disclosures of her health information, the covered entity should communicate those restrictions to law enforcement officials. Informing law enforcement of the restrictions would help investigators understand a victim's safety concerns. Law enforcement officials would then be better prepared to help the victim seek protection during the investigation.

I. Directory Information

Because directory information includes the name, location and condition of the patient, a perpetrator could easily locate a victim to commit further violent acts. While individuals who are not incapacitated would have an opportunity to opt out or limit the amount of information to be disclosed, incapacitated individuals would have no protection. A provider who reasonably believes that the injuries of an incapacitated individual could be the result of domestic violence should be prohibited from disclosing the location of the individual. We believe that such a limitation is essential for the safety of domestic violence victims. Providers should be given discretion to disclose the location of the individual to immediate family members who qualify as next of kin *and* when the provider does not believe the injuries could be a result of domestic violence.

J. Notice of Information Practices

We encourage the Secretary to require entities to make reasonable efforts to obtain a signed acknowledgment that the individual has received and read the notice of information practices. While we believe that a signed authorization is the best policy, we also believe that a signed acknowledgment could also serve as an "initial moment." (See Treatment, Payment and Health Care Operations)

K. Next of Kin

We are very concerned about situations where a perpetrator who is a next of kin attempts to obtain information about his victim's treatment for her injuries. If the perpetrator discovers that the victim discussed her injuries and identified the perpetrator by name, he could confront the victim. This confrontation may be another violent episode. We strongly believe that where verbal agreement cannot be obtained any disclosure must take into consideration whether the information could jeopardize the safety of the victim.

We are also concerned that the proposed rule does not have adequate verification procedures to identify those who are requesting information. If verbal agreement is not possible, the perpetrator could easily obtain domestic violence information. In the Secretary's preamble (p. 59972), she states that when there is no verbal agreement, a verbal inquiry into the identity of the person requesting the information is sufficient. We strongly disagree and believe that an entity should verify the identity of the next of kin who has requested the information. A perpetrator could attempt to obtain information as next of kin while the victim is unconscious in order to find out whether she previously identified him as the perpetrator. By verifying the identity of the person requesting the information, a provider could then make an informed decision as to whether the safety of the victim may be jeopardized.

L. Right to Restrict

We recommend that the Secretary's proposed right to request restrictions on all information be retained. However, a mere right to request restrictions does not adequately address the safety concerns of victims of domestic violence or the discrimination and safety concerns of others with sensitive health conditions. Victims of domestic violence have immediate safety concerns when information about their treatment is disclosed to the perpetrator. Often perpetrators are angered if they find out that their victims have told a provider about the abuse. As a result, the victim may be in more serious danger of personal harm. There are many ways for perpetrators to discover that the victim has had or is seeking medical attention, or discover the whereabouts of the victim (i.e. by finding a bill or explanation of benefits or notice of appointment in the mail, answering medical history questions posed by an attending health care worker or an insurer, directly asking a provider or insurer, or by false pretenses). The victim should be able to request that, to the extent possible, covered entities not use or disclose protected health information in ways that would alert the perpetrator. Thus, the victim should be able to request that a bill be sent to a different address, or that the perpetrator (if identified) not be given particular health information about the victim, or that only specified persons be given full access to the patient's health information. Not requiring that entities restrict use of information has broad effects. If victims of domestic violence are not adequately assured of the confidentiality of their information, they will be less likely to seek medical attention and counseling. Failing to give victims a true right to limit disclosures of their health information where the disclosure would endanger their safety undermines the efforts of the health care community to serve victims and deprives victims of necessary care and assistance.

We appreciate the Secretary's concern about the unworkability of an absolute right to restrict, but when restrictions concern information that could jeopardize the patient's safety, the safety of the individual outweighs any administrative burden. While restrictions may be ignored or overlooked because the person handling the information is unaware of the restrictions, we believe that entities could minimize any oversight by flagging restricted information in a noticeable place and manner on the information itself. All entities who receive sensitive information subject to restrictions by the individual should be informed of and comply with the restrictions.

We are very concerned that the Secretary's proposed rule does not permit individuals to request restrictions on the use and disclosure of information in emergency situations. We strongly believe that the right to restrict should apply in emergency situations. A victim who has been harmed by violence may first turn to emergency services for aid, and the victim should be able to request that the perpetrator not be told of her condition or whereabouts.

M. Inspection and Copying

We recommend that the rule grant covered entities broader discretion to deny access to protected health information in certain circumstances where necessary to protect minors and other vulnerable people (elders, or those who are incapacitated or incompetent) from abuse by their parents, guardians, persons acting in loco parentis, or legal representatives who seek information under section 164.514. Extra protection is necessary for vulnerable people who depend on others to exercise their rights under the regulations, but who must be shielded from those empowered to act in their stead. Health care professionals who treat victims of child abuse, elder abuse, and other forms of domestic violence should have the discretion to withhold information about their patients from those whom the professional reasonably believes may harm the patient. Such discretion is critical when the patient has revealed the abuse and physical or emotional retaliation by the abuser is a real possibility.

V. CONCLUSION

While we have many concerns with the proposed regulation, we believe that the rule provides greater privacy protections than exist today. We strongly encourage Congress to take the important next step by filling the gaps left by HIPAA.

Statement of Health Industry Manufacturers Association

This testimony is submitted on behalf of the Health Industry Manufacturers Association (HIMA) and its 800 member companies. HIMA is the largest medical technology trade association in the world, representing manufacturers of medical de-

vices, in vitro diagnostic products and health information systems. HIMA member companies supply nearly 90 percent of the $68 billion of health care technology products purchased annually in the United States and more than 50 percent of the $159 billion purchased annually worldwide. We welcome the opportunity to submit testimony for the record on issues surrounding the privacy of individually identifiable health information.

Comments on the Proposed Privacy Regulation

Medical technology encompasses thousands of life-saving and life-enhancing products used by more than 50 medical specialties in numerous procedures and applications. Through advances in medical technology, more lives are saved, illnesses are prevented and recovery times are shorter.

Medical device innovation differs significantly from pharmaceutical development in that most devices on the market today result from a series of incremental improvements to preexisting devices. These improvements result from continued vigilance by the manufacturer and substantial input from the provider community. Although well-designed research plays a significant role, formal research projects must be complemented by one-to-one interaction between the researchers tasked with developing and improving a technology and the clinical personnel who use it in their therapeutic and diagnostic interactions with patients. Continuity and perseverance in research and the ability to communicate freely with caregivers and patients are key drivers of innovation.

HIMA strongly supports the development of reasonable patient confidentiality standards. We recognize the difficulties associated with developing privacy standards as highlighted by the Department of Health and Human Services (HHS) in the Background section of the preamble to the proposed rule. HHS has made a considerable effort toward ensuring that patient safety, the quality of care and medical research are not adversely affected by this regulation. Nevertheless, we believe the proposed rule still has many shortcomings. There are numerous requirements that are unrealistic and will not meet the needs of a health care system that is far more complex than that contemplated by the proposed regulation or the statute. Many items are ambiguous or require much more explanation and clarification.

Taken together, these factors create concern from our perspective about the safety and quality of patient care, and our ability to collect data to support medical research. We believe these problems must be addressed in a satisfactory manner before any final regulatory framework is implemented.

We are pleased to share with the Subcommittee our concerns about the proposed HHS privacy regulation. These are:

The Definition of Covered Entity Should Exclude Most Device Manufacturers

We are extremely troubled that the proposed rule does not clarify that the vast majority of device manufacturers are not covered entities. As currently drafted, the definition of covered entity includes device manufacturers who act as Medicare suppliers. These types of companies comprise a very small portion of the medical device industry. Because the definition of a covered entity does not distinguish between the majority of device manufacturers and the ''supplier manufacturers,'' it has the potential to be misinterpreted by implying that device manufacturers, in general, are covered entities.

The rule is also vague in cases where a ''supplier manufacturer'' has only one part of its business that acts as the ''supplier.'' Thus, in addition to urging HHS to clarify that the vast majority of device manufacturers are not intended to be covered entities under the rule, we have urged more detail regarding the scope of the supplier component and its relationship to the rest of the company's business.

Requirements to ''Deidentify'' Individual Health Information are Unworkable

We believe the rule's requirement that 19 identifiers be removed before protected health information can be considered ''deidentified'' is unworkable and will yield information which in most cases is useless for research purposes. Additionally, the proposed rule deviates from the ''reasonable basis'' standard promulgated by the Health Insurance Portability and Accountability Act (HIPAA) and instead adopts a standard which will be very difficult to meet, where one must, in effect, demonstrate that there is ''no reason to believe'' that a recipient of protected health information could ''reidentify'' the recipient.

In light of HIPAA's civil and criminal provisions, it is likely these requirements, if adopted, will severely impede medical research by creating an atmosphere of extreme uncertainty surrounding what data can be legitimately released by a covered entity. We have urged HHS to adopt the HIPAA standard regarding individually

identifiable health information. This will allow health information to be used unless there is a reasonable basis to believe that the information can be used to identify the individual.

The Definition of Public Health Authority Must Be Expanded

The proposed rule has a severely limited definition of public health authority. Medical device manufacturers operate in a global environment. As such, device manufacturers must provide protected health information not only to U.S. government entities, but also to government entities in other countries as well as private organizations. It is critical, therefore, that the definition of public health authority be expanded to allow disclosures to foreign governments and private sector organizations.

Device Manufacturers Should Be Permitted to Support Treatment and Diagnosis

The proposed rule does not permit manufacturers to support providers with treatment or diagnosis where protected health information may be disclosed. As a result, patient care may be jeopardized and access to life-saving and life-enhancing technologies may be seriously delayed.

Device manufacturers frequently assist providers with the operation and use of a particular device or customize devices for particular patients. In many cases, the Food and Drug Administration (FDA) requires these activities and thus would be permitted by the proposed rule. Occasionally, however, a provider may ask a manufacturer for support that is not required by FDA, an activity not permitted by the proposed rule. In these instances, and in order to assure appropriate patient care or speedy patient access to needed devices, the regulation should allow a provider to disclose protected health information without individual authorization to the manufacturer.

Device Manufacturers Should Be Permitted to Train Providers

Frequently, device manufacturers are the only entities with the knowledge and experience to train providers on the use of a device. In addition to written instructional materials, such training frequently includes one-on-one tutorials in which the needs of individual patients are necessarily addressed. As currently written, the proposed regulation prohibits this type of provider training unless patient authorization is obtained, although the rule permits similar types of training if it is provided by health care professionals.

To ensure the continued safe and proper use of medical devices, we have urged HHS to change the proposed rule to reflect that effective medical education results from a variety of sources including medical device companies and that this type of training should be permissible without patient authorization.

The Proposed Rule Will Discourage the Collection of Needed Public Health Information

The proposed rule permits disclosure of protected health information to device manufacturers when the information is needed to comply with rules or other directions of a governmental authority. However, the proposed rule lists only one requirement, device tracking, as an example. The device industry must comply with hundreds of FDA requirements that require the disclosure of protected health information.

Given the severe civil and criminal penalties which will apply to entities violating the confidentiality standards established by the rule, we are gravely concerned that an atmosphere may develop where hospitals and other providers who now freely provide needed information to device manufacturers, will be reluctant to provide that same information in the future.

To ensure that medical device manufacturers can carry out the activities mandated by FDA and other government agencies that require protected health information without individual authorization, it is essential that the final rule enumerate the many requirements with which device manufacturers must comply.

Device Manufacturers Should Be Permitted to Support Data Collection Activities of Governmental and Private Entities

The proposed rule permits disclosure of protected health information to a government health data system used to collect data for analysis in support of policy, planning, regulatory or management functions authorized by law. Government (specifically the Health Care Financing Administration (HCFA)) as well as private payers often rely on device manufacturers to supply this information specifically to support reimbursement and coverage policies.

We believe the rule should allow device manufacturers to collect protected health information that will be used to support HFCA's reimbursement policies and other

related decisions. The rule should also allow device manufacturers to collect the same information for third party payers who, in turn, must supply device reimbursement information to HCFA.

The Proposed Requirements for Research Invalidate the Common Rule

Finally, the proposed rule establishes new criteria to be included in patient consent forms for participation in medical research which conflict with current law governing human participation in clinical trials and which are inappropriate for medical device trials.

Currently, the form and content of patient authorizations to participate in medical device trials are established by Institutional Review Boards acting in accord with the federal regulatory framework for the protection of human subjects (known as the Common Rule). The proposed rule invalidates a number of the elements required by the Common Rule. Additionally, a number of the elements in the proposed form are confusing and inappropriate for medical device clinical trials and the volunteers who participate in them.

Conclusion

In conclusion, HIMA strongly supports measures that will ensure that individual health information is appropriately protected while maintaining the safety and quality of care through necessary communications and procedures. We believe the proposed privacy rule has a number of shortcomings that will impede important research needed to support device innovation and patient access to new and improved medical technologies. We look forward to workable solutions that will guarantee safe patient access to innovative technologies through mechanisms that promote medical research and quality of care.

Statement of Daniel V. Yager, LPA, Inc.

Mr. Chairman and Members of the Subcommittee:

Thank you for allowing us to present our views to your Subcommittee regarding the proposed medical privacy regulations issued by the Department of Health and Human Services on November 3, 1999, "Standards for Privacy of Individually Identifiable Health Information." LPA, is a public policy advocacy organization representing senior human resource executives of more than 250 of the largest corporations doing business in the United States. LPA's purpose is to ensure that U.S. employment policy supports the competitive goals of its member companies and their employees. Collectively, LPA member companies employ more than 12 million employees, or 12 percent of the private sector workforce.

Although perhaps not intended by the Department of Health and Human Services (HHS), LPA believes that the proposed medical privacy regulations could arguably prevent employers from conducting drug testing and fitness for duty testing and from requiring employees to provide Family and Medical Leave Act certifications as permitted under current law. On February 15, 2000, LPA filed comments with HHS detailing our concerns, based upon based upon extensive discussions with LPA member companies.

LPA's comments underscore the critical role played by drug testing in promoting workplace safety and reducing medical and workers' compensation costs. The comments note that 70% of all employers conduct drug testing. Even HHS conducts drug testing before hiring its criminal investigators. LPA believes that it is important that the final medical records confidentiality regulations encourage, rather than discourage, employers to engage in drug testing, even if the testing is not required by federal law.

The comments also point out that fitness for duty tests are already subjected to extensive restrictions under the Americans with Disabilities Act (ADA), which requires employers to keep all employee medical records confidential. The ADA also regulates when an employer may require an employee or prospective employee to take a fitness for duty test and which supervisors may view the results of the test. Because such tests confirm whether an employee is physically and mentally capable of handling dangerous tasks, they have the added benefit of ensuring that employers are providing a workplace free from recognized hazards under the Occupational Safety and Health Act. LPA believes that the regulations should clearly exclude fitness for duty tests.

Similarly, employers may require employees to provide medical certifications under the Family and Medical Leave Act (FMLA) to ensure that the employees use the federally-mandated leave for proper purposes. Although the regulations may im-

pact an employer's administration of the FMLA less severely than drug testing programs and fitness-for-duty testing under the ADA, LPA has urged the Department of Health and Human Services to clarify that these certifications would not be impacted by the final regulations.

Mr. Chairman, LPA believes that medical records used for human resources purposes are already substantially protected by employment laws. We urge the subcommittee to voice its strong opposition to the additional restrictions in the regulations that would only serve to make an employer's compliance with existing laws more difficult without bolstering employee protection. A complete copy of our comments is attached for your information.

February 15, 2000

U.S. Department of Health and Human Services
Assistant Secretary for Planning and Evaluation
Attn: Privacy-P, Room G–322A
Hubert H. Humphrey Building
200 Independence Ave., SW
Washington, DC 20201

RE: Standards for Privacy of Individually Identifiable Health Information

To Whom It May Concern:

We are writing to express our strong concerns regarding the application of the medical privacy regulations proposed on November 3, 1999,[1] to the ability of employers to maintain mandatory drug testing programs and to make critical employment decisions which are currently already subject to restrictions under numerous federal and state laws, including the Americans with Disabilities Act, the Family and Medical Leave Act, and the Occupational Safety and Health Act.

LPA, Inc. is a public policy advocacy organization representing senior human resource executives of more than 250 of the largest corporations doing business in the United States. LPA's purpose is to ensure that U.S. employment policy supports the competitive goals of its member companies and their employees. LPA member companies employ more than 12 million employees, or 12 percent of the private sector workforce. Because of the broad scope of the regulations as discussed below, we believe every LPA member company would be affected in a significant manner.

LPA's member companies have numerous concerns with regard to the regulations which will be expressed through their own individual comments as well as those of other organizations to which they belong. LPA does not believe the agency intended the regulations to cover an employer's use of employment-related medical information within the bounds of current law. However, the regulations are sufficiently vague that it is possible that they cover drug testing and other areas involving critical employment decisions where Congress and various state legislatures have already chosen to regulate the disclosure of health information.[2]

Our concern centers upon the broad definition of "health information" in § 160.103 to include "any information . . . that (1) Is created or received by a health provider . . . [or] . . . employer . . .; and (2) Relates to the past, present, or future physical or mental health or condition of an individual. . .." This definition arguably could be broad enough to include:

- data compiled pursuant to a mandatory drug testing program maintained by an employer as a condition of employment for its employees;
- data compiled pursuant to a fitness for duty test conducted in accordance with the Americans with Disabilities Act to provide a reasonable accommodation or to ensure that an individual is capable of performing strenuous or difficult work; and
- information contained in a certification provided by an employee as a condition to his or her entitlement to medical leave pursuant to the Family and Medical Leave Act.

LPA does not believe the agency intended to limit these activities. However, because the proposed regulations cover "protected health information," which essentially means electronically transmitted health information that identifies a particu-

---

[1] Standard for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (proposed Nov. 3, 1999).

[2] LPA agrees with the statement in the Preamble that the Secretary does not have the authority under the Health Insurance Portability and Accountability Act to regulate the use of protected health information once it is disclosed to employers. See *id.* at 59,923. As is detailed in this letter, employer use of such information is already substantially regulated by existing law.

lar individual, the regulations would appear to govern electronically transmitted information used for the purposes listed above. LPA believes that the final regulations should clearly exempt these uses from their scope, both for compelling public policy reasons and because they are adequately regulated by existing employment laws. Each of these concerns will be discussed separately below.

I. Mandatory Drug Testing Programs

Many employers implement drug testing of prospective and current employees to ensure that their employees do not pose a threat to themselves, their co-employees, or the public at large. Indeed, federal agencies are required to test applicants and employees in sensitive positions for drugs under Executive Order 12,564,[3] which implements a drug-free federal workplace. A review of federal agency web site job postings reveals that drug testing is a prerequisite for individuals seeking certain federal jobs, such as those who apply as criminal investigators in the Department of Health and Human Services[4] and communications equipment specialists for the Federal Aviation Administration.[5]

Likewise, private sector employers have used drug testing programs for years to enhance workplace safety, particularly when the jobs involve hazardous activities such as manufacturing or transportation. The most recent statistics indicate that 70 percent of all employers test their employees for drugs.[6] Employers have implemented workplace drug testing for a variety of reasons, including to enhance workplace safety, maintain product quality, productivity and employee morale, and reduce medical and workers' compensation costs.[7]

Overall, workplace drug use is estimated to cost employers over $100 million annually.[8] The anecdotal evidence of the effectiveness of workplace drug testing programs is "compelling" according to the U.S. Department of Labor's Internet site. For example:

- drug-using employees at GM average 40 days sick leave each year compared with 4.5 days for non-users;
- employees testing positive on pre-employment drug tests at Utah Power & Light were 5 times more likely to be involved with a workplace accident than those who tested negative;
- in Ohio, the establishment of drug-testing and treatment programs reduced on-the-job injuries by 97 percent;
- Southern Pacific Railroad experienced a 71 percent decrease in injuries;
- a manufacturer with 560 employees reduced industrial accidents over thirty percent.[9]

Thus, there is ample evidence that drug testing helps achieve vital workplace goals.

Because of the success of programs like these, testing in some industries is now even required by law, such as the mandatory drug testing programs for commercial drivers required by the Omnibus Transportation Employee Testing Act of 1991.[10] Even where drug testing is not required, it is often encouraged. Thus, the Drug-Free Workplace Act of 1988[11] requires all federal contractors with contracts of at least $25,000 to certify that they are providing a drug-free workplace, at the risk of contract debarment if they fail to do so. Many contractors are able to provide this certification as a result of their drug testing programs.

The regulations effectively appear to encompass information generated by mandatory drug testing. The medical profession holds a longstanding belief that drug dependency is a disease to be treated, rather than a disability to be accommodated.[12] However, if that is the case, then workplace drug testing, despite an employer's de-

---

[3] Exec. Order No. 12,564, 51 Fed. Reg. 32,889 (Sept. 15, 1986) *reprinted in* 5 U.S.C.A §7301 (note) at 166–70 (1996).

[4] Department of Health and Human Services, Job Announcement for a Supervisory Criminal Investigator, announcement number OIG–00–001, *available at* http://www.psc.gov/spo/oig0001.shtm1.

[5] Department of Transportation, Federal Available Administration, Airway Transportation System Specialist announcement, *available at* http://jobs.faa.gov/anndetail.sap?vac__id=47575.

[6] American Management Association, 1999 AMA Survey on Workplace Testing, at 2.

[7] *See e.g.*, G. John Tysse and Garen E. Dodge, WINNING THE WAR ON DRUGS: THE ROLE OF WORKPLACE TESTING, 147(1989)

[8] Department of Labor Internet Site: "Working Partners for an Alcohol and Drug-free Workplace, Background Information: Workplace Substance Abuse," *available at* http://www.dol.gov/dol/asp/public/problems/drugs/backgrnd.htm.

[9] *Id.*

[10] 49 U.S.C.A. §20103.

[11] 41 U.S.C.A. § *et seq.* (West 1987 & Supp. 1999).

[12] *See, e.g.*, American Medical Assn., Drug Dependencies As Diseases, House of Delegates Resolution H–95.983 (Jan. 1998) *available at* http://www.ama-assn.org/apps/pf__online/pf__online.

sire to maintain a safe workplace, is covered under the proposed regulations' definition of health care, which includes "preventive, diagnostic . . . rehabilitative . . . care, counseling, service or procedure with respect to the physical or mental condition, or functional status of a patient."[13]

Because it is important that employers be able to continue to maintain mandatory drug testing programs, Congress excluded them altogether from the strict requirements of the Americans with Disabilities Act governing medical examinations.[14] The exclusion of mandatory drug testing programs from the ADA requirements made sound policy sense—to encourage workplace drug testing. However, the exclusion also logically flowed from the fact that such programs seek to obtain information about the deliberate illegal activities of individuals that could have serious work consequences, even if those activities were the result of a disease that is beyond their control.

The same considerations that led Congress to exclude testing for the illegal use of drugs from the strict regulation of medical examinations under the Americans with Disabilities Act should lead to the same exclusion from the proposed regulations.

II. Fitness for Duty Testing

Many jobs require certain levels of physical and/or mental competencies. Fitness for duty examinations allow employers to determine whether an individual can perform the essential functions of the job and, if they are not able to because of a disability, whether a reasonable accommodation can be made to enable them to perform those functions. Likewise, fitness tests for safety purposes confirm that an employee is physically and mentally capable of handing dangerous tasks. Each of these similar but distinct situations is dealt with below.

The Equal Employment Opportunity Commission, in its January 1992 "Technical Assistance Manual on the Employment Provisions (Title I) of the Americans With Disabilities Act," provides several examples of fitness tests, all of which are consistent with the ADA's protections:

- ensuring that "prospective construction crane operators do not have disabilities such as uncontrolled seizures that would pose a significant risk to other workers;"[15]
- testing of workers in certain health care jobs "to ensure they do not have a current contagious disease or infection that would pose a significant risk of transmission to others;"[16] and
- ensuring that an individual considered for a position operating power saws or other dangerous equipment is not someone "disabled by narcolepsy who frequently and unexpectedly loses consciousness."[17]

Under the Americans with Disabilities Act, employers are already substantially regulated as to when they can require medical exams of, or request medical information from individuals; what they can examine or ask them for; and what employment decisions are permissible once medical information concerning the individual is acquired. An employer is generally prohibited from discriminating against a "qualified individual with a disability," which means a disabled individual who can perform the "essential functions of the job" with or without a "reasonable accommodation."

The ADA correctly recognizes that the employer must have access to a certain amount of medical information about employees and prospective employees to comply with the law. Under Section 102 of the ADA, employers have the right to require a medical examination after an offer of employment has been made and prior to the commencement of employment.[18] If, during the medical examination, the doctor discovers a condition that may affect the person's ability to do the job, the employer still must go through the "reasonable accommodation process" to determine whether the individual could do the essential functions of the job with a reasonable accommodation.[19] Once the individual has been hired, the employer may not require medi-

---

[13] 64 Fed Reg. 60,049 (to be codified at 45 C.F.R. §160.103).

[14] "For purpose of this subchapter, a test to determine the illegal use of drugs shall not be considered a medical examination." 29 U.S.C.A. §12114(d)(1) (West 1999).

[15] U.S. Equal Employment Opportunity Commission, Technical Assistance Man., Title I, Americans with Disabilities Act, *reprinted in* Americans With Disabilities Act Man. 90:0556 (BNA)(1992).

[16] *Id.*

[17] *Id.* at 90:0543.

[18] 42 U.S.C.A. §12112(d).

[19] 42 U.S.C.A. §12111(9).

cal examinations unless they are "job-related and consistent with business necessity."[20]

Meanwhile, the ADA limits the amount of medical information that can be obtained during employment to that information which is job-related and consistent with business necessity. Strict confidentiality requirements apply to the information, and several courts have held, with agreement from the Equal Employment Opportunity Commission, that these requirements apply regardless of whether an individual has a disability.[21] During the hiring process, the employer may share medical information only with decision-makers with a "need to know" the information. Even an employee's supervisor and manager are not entitled to any medical information beyond what limitations the employee has to do the particular job. Thus, the ADA already protects against any improper use of critical medical data by the employer.

Yet, the data obtained consistent with ADA requirements would appear to constitute "health information" under the proposed regulations, even though HHS probably did not intend this result. Thus, even though the employer would have a narrow right to access the data under the ADA, a new authorization requirement would be superimposed by the proposed regulations. As a result, employers could be forbidden from viewing the results of medical exams taken to detect or confirm the existence of a disability that could affect the ability of an employee to do his or her job competently and safely.

This restriction has implications beyond the ADA. Results of fitness for duty tests performed in accordance with the ADA may also be used to ensure an employer is complying with the Occupational Safety and Health Act (OSH Act). Although fitness for duty tests are not required by the OSH Act,[22] employers may reduce unnecessary workplace accidents by implementing these tests because they will identify employees who are impaired, physically incapable, or not properly trained and ensure that they are not placed in jobs involving hazardous work.[23] However, the medical regulations are probably sufficiently vague that the information gathered under these tests would not be exempted under them, even though fitness testing is consistent with the purpose of the OSH Act.

In addition, the OSH Act specifically requires employers to provide voluntary medical testing for its employees. An employer could use the information received to comply with its general obligation under OSHA to provide a place of employment that is free from hazards. However, it would appear that the information gathered under these tests would not be exempt from the medical privacy regulations and therefore it could be subjected to numerous restrictions that would prevent the use of the data for the very purpose that it was intended.

For the foregoing reasons, we recommend that the final regulations make clear that they will not apply to information regarding fitness tests that an employer or its agents may lawfully obtain, use or disclose under the ADA, state and local laws relating to discrimination on the basis of disability, the OSH Act, and state safety and health laws. Use of such information is already adequately protected under the ADA, and additional consent and disclosure requirements would serve to impede the administration of federal antidiscrimination policy.

III. Family and Medical Leave Act

Under the Family and Medical Leave Act (FMLA), employees are guaranteed a right to up to twelve weeks of leave annually for a serious medical condition. Under Section 103 of the FMLA, employees who wish to use FMLA medical leave can be required by their employer to provide a certification issued by a health care provider that discloses, in part:

- the date on which the employee's "serious medical condition" began;
- the probable duration of the condition;
- the "appropriate medical facts within the knowledge of the health care provider" regarding the condition; and

---

[20] 42 U.S.C.A. §12112(d)(4)(A).

[21] *See Roe v. Cheyenne Mt. Conf. Resort*, 124 F.3d 1221 (10th Cir. 1997), *cert. denied*—U.S.—, 119 S. Ct. 1455 (1999); *Criffen v. Steeltek, Inc.*, 160 F.3d 591 (10th Cir. 1998); *Cossette v. Minnesota Power & Light*, 188 F.3d 964 (8th Cir. 1999); *Fredenberg v. Contra Costa County Dept. of Health Services*, 172 F.3d 1176 (9th Cir. 1999).

[22] The OSH Act requires employers to provide employees "employment and a place of employment that is free from recognized hazards which. . .are likely to cause death or serious physical harm to his employees." 29 U.S.

[23] Although hazard avoidance is often employer-driven "[i]n many workplace situations, avoidance of hazards depends on proper employee conduct. Many citations have been issued under the general duty clause either because actions of employees created hazards or because employees did not take precautions to avoid hazards." Stephen A. Bokat and Horace A. Thompson III, Eds., OCCUPATIONAL SAFETY AND HEALTH LAW, 136 (1988).C.A. §654(a) (West 1999).

• a statement that the employee is unable to "perform the functions of the position."[24]

Medical certifications provided by employees returning from leave under the Family and Medical Leave Act allow employers to ensure that the employee is ready to undertake the duties required in the employee's position. Similar issues exist with respect to the information included in the opinion of a second health care provider requested by an employer who doubts the validity of the employee's initial certification[25] or in the opinion of a third health care provider called upon to resolve a conflict between the opinions of the first and second health care providers.[26]

Much of the information contained in the medical certification would appear to meet the definition of protected health information under all the proposed bills, and would therefore be covered by the requirements of those bills. However, under the FMLA, the employer may require the employee to provide a medical certification before returning the employee to his or her job. Thus, there is an implicit requirement that the employee provide consent for the employer to see the medical certification.

To avoid any inadvertent conflicts between employment law and the medical privacy regulations, we recommend that the final regulations exclude protected health information contained in certifications that an employer or its agents may use or disclose when exercising their rights or responsibilities under the FMLA.

IV. Consequences of an Employee's Refusal to Provide Authorization

In addition to recognizing that an employee authorization is not required where employers are currently permitted to use protected health information, the regulations should state that an employer is permitted to make an employment decision based on an employee's refusal to provide the results of a drug or a fitness-for-duty test under the ADA, FMLA, and similar laws. This would make the regulations consistent with the existing application of these laws and eliminate potential confusion regarding application of the exclusion.

A few examples illustrate the need for such a provision. The ADA acknowledges that an employer is not obligated to hire an employee with or without a disability who is not able to perform the essential functions of the job. If an employee refuses to submit to a post-offer fitness for duty test, or refuses to disclose the results of such a test, the ADA allows the employer to refuse to hire the employee because the employer cannot assess whether the employee can perform the job's essential functions.

An employer faced with the potential that an unskilled or untrained employee could be placed in a safety sensitive position and could cause substantial safety problems, must determine the employee's fitness before they are assigned such a position. Thus, an employer should be allowed to take appropriate action against an employee who refuses to take or disclose the results of a drug or fitness test that could result in safety implications.

Similar reasoning applies under the FMLA and more generous employer-provided leave policies. As noted above, an employer may require an employee to provide a medical certification and is not required to restore the employee to his or her position until the certification is provided. Thus, if an employee refused to provide the disclosure, the employer could refuse to reinstate the employee.

Moreover, employers often provide benefits beyond those required by the federal employment law. For example, in addition to providing unpaid leave under the FMLA, many employers also provide sick leave for short absences and temporary disability benefits for longer-term medical absences. For this reason, LPA also recommends that the regulations should permit employers to require employees to provide certifications of their conditions to demonstrate eligibility for these employer-provided benefits. The same rationale applies to both situations—in order to receive the protection of the law or voluntary benefits provided by the employer, the employee must demonstrate that he or she had a bona fide condition that triggered the protection or the benefits.

By acknowledging that employers may make employment decisions based on an employee's refusal to take or disclose the results of a mandatory drug or fitness for duty test, a certification for FMLA or employer-provided paid leave, the regulations would protect the ability of employers to comply with existing labor and employment laws, maintain the safety of their workplaces, and offer generous leave packages.

---

[24] 29 U.S.C.A. §2613(b)(1–4) (West 1999).
[25] *Id.* at §2613(c) & (d).
[26] *Id.* at §2613(e).

V. Limitation to Electronic Data

As proposed, the medical privacy regulations only apply to electronically transmitted protected health information. However, the Secretary argues in the Preamble that she has the authority to regulate paper records under several authorities.[27] LPA takes exception to this statement. The Health Insurance Portability and Accountability Act (HIPAA), which authorized the regulations, clearly does not authorize the Secretary to regulate anything but electronically transmitted information. This is made clear in the legislative history as well.[28] LPA opposes the Secretary's stretched attempt to expand her authority beyond that which she is expressly granted in HIPAA.

Thank you for this opportunity to submit our views.

Sincerely yours,

DANIEL V. YAGER
Senior Vice President and General Counsel

Statement of Medical Group Management Association

Medical Group Management Association (MGMA) urges the Department of Health and Human Services (HHS) to re-issue the proposed privacy rule. "MGMA appreciates the enormous complexities that HHS was confronted with in drafting the proposed rule to protect the confidentiality of medical information. In light of the extensive revisions that HHS should incorporate into a final rule, MGMA urges HHS to issue a new proposed rule reflecting the revisions before it drafts a final rule. Due to the importance and overarching impact of this issue, all interested parties should have an adequate opportunity to review and comment on the changes to the original proposed rule," according to MGMA President and CEO William F. Jessee, M.D.

The privacy of an individual's personal health information should never be inappropriately compromised. However, MGMA contends that protecting the privacy of medical information must be balanced against the unnecessary burdens privacy protections place upon group practice administrators and all health care providers. Furthermore, it is essential that privacy protections do not interfere with vital activities such as medical treatment and research.

"MGMA commends the efforts of HHS to protect the confidentiality of medical information. MGMA believes HHS took several positive steps in addressing a very difficult issue. However, we also believe there are several significant flaws in the proposed rule, which would place tremendous burdens on medical group practices and interfere with the delivery of efficient and high quality health care," said Jessee.

In light of the limited applicability of the proposed rule mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), MGMA maintains that the best avenue for protecting health information is through comprehensive legislation. MGMA is concerned that the proposed rule would not apply to many entities that use and disclose medical information on a daily basis (e.g., life insurance issuers, third-party administrators, and employers). Furthermore, the protections provided in the proposed rule would not cover purely paper records.

In its formal submission to HHS, MGMA emphasized the following:

- **Provided HHS has the authority, MGMA urges HHS to expand the rule to cover all information, even information that has never been electronically maintained or transmitted.** There are many medical organizations, especially small physician practices, that still maintain and transmit information in paper form. In order to protect fully the confidentiality of health information, HHS should apply its standards to all information, regardless of how it is stored or transmitted. In addition, the proposed approach would create an undesirable and confus-

[27] Although we are concerned that extending our regulatory coverage to all records might be inconsistent wit the intent of the provisions of HIPAA, we believe that we do have the authority to do so and that there are sound rationale for providing a consistent level of protection to all individually identifiable health information held by covered entities." *Id.* at 59,924.

[28] U.S.C.A. §1320d–2 (West Supp. 1999), "The Committee recognizes the role of the private sector in establishing innovative data transactions systems relating to electronic exchange. . .privacy standards, and electronic signatures. The standards adopted would protect the privacy and confidentiality of health information. Health information is considered relatively 'safe' today, and because it is secure, but because it is difficult to access. These standards improve access and establish strict privacy protections." Conference Report on the Health Insurance Portability and Accountability Act of 1996, H. Rep. No. 104–406 at 99 (1996), *reprinted in* 5 U.S.C.C.A.N. 1,900 (1996).

ing scenario involving "mixed" records with certain records potentially containing both protected and unprotected information. This would place administrative burdens upon providers and administrators to ensure that protected health information is handled appropriately.

• **MGMA supports the approach adopted by HHS in the proposed rule that would not require a patient's authorization to use or disclose protected health information (PHI) for treatment, payment, and "health care operations."** Patients expect that their health information will be used for treatment and payment when they seek medical care. Requiring an authorization would be a mere formality and not serve a legitimate purpose, since an authorization often is obtained prior to a patient receiving medical care. MGMA strongly believes that a separate authorization should not be required for health care operations, since these activities are directly related to and often times inseparable from treatment and payment.

• HHS proposes that a covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure. **While the intent behind "minimum necessary" is commendable, MGMA believes this standard places an unfair burden on the entity making a disclosure and may interfere with patient care as well as patient safety initiatives.**

• **While MGMA recognizes the importance of protecting the privacy of health information in all hands, we strongly object to the "business partner" proposal and recommend that HHS completely remove the liability provision of the proposed rule.** It is impractical and unrealistic to expect a covered entity to monitor and determine if a business partner is complying with the requirements of the regulation. In addition, as outlined in the rule, an individual could sue a covered entity if a business partner inappropriately discloses information. However, HIPAA does not extend to HHS the authority to include a "private right of action," and MGMA believes HHS is attempting to circumvent the statute through the business partner proposal.

• **MGMA strongly supports the principle of "scalability," which provides practices flexibility in complying with the proposed rule's requirements.** MGMA applauds HHS for recognizing the fact that the magnitude and complexity of the proposed rule will create significant monetary and administrative burdens.

The full text of MGMA's formal comments on the proposed rule is posted on the Public Policy section of MGMA's website at *"http://www.mgma.com/legislation/*. For specific questions regarding MGMA's comments, please contact Aaron N. Krupp, MGMA Government Affairs Representative, at (202) 293–3450.

Founded in 1926, MGMA's membership includes more than 7,100 organizations, representing more than 185,000 physicians. MGMA executive offices are in Englewood, Colo.

NATIONAL ASSOCIATION OF
INSURANCE COMMISSIONERS
WASHINGTON, DC 20001
March 1, 2000

The Honorable William Thomas
Chair
Subcommittee on Health
Committee on Ways and Means
1136 Longworth House Office Building
Washington, DC 20515–6349

Dear Chairman Thomas:

The National Association of Insurance Commissioners (NAIC), representing the nation's fifty-five chief insurance regulators, submits the enclosed document and asks that it be included in the record for the hearing on health information privacy held by your subcommittee on February 17, 2000.

The enclosed document is the comment letter the NAIC sent to the United States Department of Health and Human Services regarding its proposed health information privacy regulation. The letter raises many concerns including the following:

• *Limited Applicability and Scope:*

The regulation only applies to a limited group of entities (health plans, health care providers and health care clearinghouses) and only applies to paper records.

While we recognize that HHS is limited in its authority and jurisdiction to apply the standards established in the regulation, we think the regulation should apply to a broader group of entities that use and disclose protected health information and should apply to all insurers, not just health insurers. We think the regulation should protect all forms of individually identifiable health information, both paper and electronic.

- *Preemption of State Laws:*

While we appreciate HHS' intent to create federal minimum standards, to preserve stronger state laws, and to protect certain state laws from any preemption, the NAIC membership has serious reservations about how the preemption standard used in the proposed regulation is to be implemented. The general rule is that "provisions" of state law are preempted to the extent that they are "contrary" to the federal statutory and regulatory scheme. We have found similar standards not to be very helpful in comparing state laws to federal requirements. A state must examine all its laws relating to health information privacy to determine whether or not its laws are contrary to the requirements in the proposed regulation. This in and of itself is a major project for states to undertake.

We offer a suggestion to help the operation of and to ease the administrative burden of implementing this standard. We propose that the states be given the greatest amount of flexibility in determining what the necessary scope of "provision" is when applying the general rule's contrary standard. In the regulation, HHS has recognized that states know their laws best and are best informed about how to apply their laws. The NAIC membership believes that the definition should preserve to the maximum extent possible state privacy initiatives that extend beyond the covered subject matter of the proposed regulation.

- *Determination Process:*

There are several serious flaws with this proposed process:

- First, the determination process is overly burdensome for states. Not only do states have to conduct a "contrary analysis" for all of their laws that protect health information and then submit requests for exceptions to HHS, but they also have to wait for HHS to make a determination in order for the states to enforce their laws.
- Second, the proposed regulation states that the federal standard applies until a determination is made. Cessation of state regulation in the interim will essentially leave plans unregulated until HHS makes a determination. We believe the current assumption in the proposed regulation that the federal standard applies until a determination is made should be reversed. State laws should stand until and unless HHS has determined otherwise.
- Third, the proposed regulation does not establish a time frame or deadline by which HHS has to issue a determination. We suggest that HHS revise its regulation to include a time period by which HHS has to make a determination. We also suggest that if HHS does not make a determination after a specified amount of time, then a default determination should be issued in favor of the state.
- Finally, even if states are granted an exemption from preemption through the HHS determination process, there is a three-year time limit on how long a state law is exempt pursuant to this determination. The process is quite burdensome for the states, so we question the provision requiring states to ask for a re-determination on the same laws every three years as a waste of time and resources for the states and for HHS. The time limit should be eliminated.

- *Lack of Guidance in Classifying State Insurance Laws:*

There is lack of guidance regarding state laws that are contrary to the proposed regulation but that could fall into more than one category of state laws that are exempt from preemption. State insurance laws easily could fall into several of the categories of exceptions. An example is a state law regulating health insurance plans (category one) that is more stringent than the federal regulation (category two) and requires health insurance plans to report information (category 3). We request that a clarification be included in the regulation stating that if a state law falls within several different exceptions, the state chooses which exception shall apply. The presumption should be that the state has the best knowledge of its laws and it has correctly classified its laws in the appropriate category of exceptions. We think this simple clarification statement will avert much litigation and prevent state insurance departments from having to defend endless challenges to their classification of their laws.

- *Lack of Clarity in Classifying State Insurance Department Activities:*

The proposed regulation establishes a list of exceptions to the authorization requirement, such that protected health information may be used or disclosed without

authorization in certain circumstances. However, under the HHS proposed regulation, the activities of state insurance departments fit under any one or more of the following three exceptions: (1) for disclosure to health oversight agencies for health oversight activities; (2) for disclosure for law enforcement purposes; and (3) for use and disclosure for judicial and administrative proceedings. The regulation is unclear about the role of insurance departments relative to these exceptions, and each of these exceptions has its own requirements and processes. We ask HHS to include language in the text of the proposed regulation stating that if a state insurance activity falls within several different exceptions, the state chooses which exception shall apply. In addition, we ask HHS to recognize the broad scope of legally authorized activities performed by insurance departments and to reflect those activities in the regulation.

- *Permitted Versus Required Disclosure:*

Under the proposed regulation covered entities are "permitted" but not "required" to disclose necessary protected health information to health oversight and law enforcement agencies. We believe that covered entities under investigation by a state agency should be required to provide that state agency with access to necessary health information when performing its legally mandated duties. This disclosure should not be optional. By not requiring insurers to provide state insurance departments with access to records, filings and other documents that may contain individually identifiable information, state insurance departments' ability and authority to perform their regulatory responsibilities is undermined. In addition, obtaining authorization from all of an insurer's clients for investigation of an insurer's business practices is not feasible or practical.

In addition to these concerns, the members of the NAIC would appreciate further discussions with the witnesses regarding the interaction between the HHS regulation and the privacy requirements found in the newly enacted Gramm-Leach-Bliley Act.

For insights into the NAIC's position regarding the issues surrounding proposed federal health information privacy legislation, I refer you to the testimony the NAIC submitted to your subcommittee on July 20, 1999. That testimony may be found on our website at *http://www.naic.org/1news/testimonies/index.htm*.

If you have any questions please contact Mary Beth Senkewicz at (202) 624–7790.

Sincerely,

KATHLEEN SEBELIUS,
Vice-President NAIC
Chair, Health Insurance Task Force
Commissioner of Insurance, State of Kansas

Enclosure

February 15, 2000

Margaret Ann Hamburg
Assistant Secretary for Planning and Evaluation
United States Department of Health and Human Services
Hubert H. Humphrey Building
Room G–322A
200 Independence Avenue, S.W.
Washington, DC 20201
Attention: Privacy-P

Dear Assistant Secretary Hamburg:

On behalf of the National Association of Insurance Commissioners (NAIC) Health Insurance Task Force, I hereby submit these comments on the proposed rules entitled, "Standards for Privacy of Individually Identifiable Health Information," published in the FEDERAL REGISTER on November 3, 1999 (64 Fed. Reg. 59918–60065).

The NAIC appreciates the Department of Health and Human Services' (HHS) efforts to establish standards to protect the privacy of individually identifiable health information maintained or transmitted in connection with certain administrative and financial transactions and to provide a basic level of protection to consumers. We too understand the necessity of protecting individuals' health information, and

as such, we have adopted stand-alone model privacy legislation[1] and have incorporated privacy protections in other health-related models. In general, we appreciate the flexibility afforded the states in the HHS proposed regulation.

Drafting standards that protect the privacy rights of individuals with respect to highly personal health information is a difficult task. Like you, the members of the NAIC sought to write standards that would not cripple the flow of useful information, that would not impose prohibitive costs on entities affected by the legislation, and that would not prove impossible to implement in a world that is rapidly changing from paper to electronic records. At the same time, the members of the NAIC recognized the need to assure consumers that their health information is used only for the legitimate purposes for which it was obtained, and that this information is not disclosed without the consumer's consent or knowledge for purposes that are likely to harm or offend the individual.

While there are many similarities between the NAIC Health Information Privacy Model Act and the proposed regulation, the members of the NAIC have serious concerns about the proposed regulation's impact on the ability of state insurance departments to perform their jobs and handle their responsibilities, which include protecting consumers and eliminating fraud.

I. NAIC Model in Relation to the Proposed Regulation

A. Background

The NAIC adopted its "Health Information Privacy Model Act" ("NAIC Model Act") in September 1998 (Attachment A). This model has a more narrow focus than the NAIC's "Insurance Information and Privacy Protection Model Act," which was adopted in 1980. The model act adopted in 1980 addresses the privacy of all individually identifiable information, whereas the NAIC Model Act adopted in 1998 establishes protections for all health information and for protected health information. The NAIC Model Act was developed with state regulators, representatives of the insurance and managed care industries, and representatives from the provider and consumer communities. Our model was developed to assist the states in drafting uniform standards for ensuring the privacy of health information.

B. *Similarities*

The HHS proposed privacy regulation addresses many of the same issues as the NAIC Model Act. Both the NAIC Model Act and the proposed regulation establish procedures for the treatment of all health information and additional specific rules for protected health information. They are similar in their basic structures and the rights conveyed to individuals regarding their health information.

In terms of structure, the NAIC Model Act and the regulation prohibit entities from using or disclosing health information except as authorized by the patient or as specifically permitted by the Act or regulation. (HHS Proposed Regulation § 164.506(a); NAIC Model Act § 10A). When protected health information is used or disclosed, both limit the amount of information used or disclosed to that amount which is necessary for the stated purpose. (HHS § 164.506(b)(1); NAIC § 10). They both establish exceptions to the authorization requirement, and many of the exceptions to the authorization requirement in the NAIC Model Act fall under what the HHS proposed regulation defines as treatment, payment or health care operations. (HHS § 164.510; NAIC § 11). The NAIC Model Act and the proposed regulation place administrative requirements on their applicable entities (HHS § 164.518, 164.520; NAIC § 5), and both establish civil and criminal penalties for violations (HHS § 164.522; NAIC § 15).

In terms of individuals' rights regarding their protected health information, the NAIC Model Act and the proposed regulation guarantee similar rights. These rights include: (1) the right to inspect and copy the individual's protected health information (HHS § 164.514; NAIC § 7); (2) the right to amend and correct the individual's protected health information (HHS § 164.516; NAIC § 8); (3) the right to receive notice of an entity's privacy practices (HHS § 164.512; NAIC § 6); (4) the right to receive an accounting of everyone to whom protected health information was disclosed (HHS § 164.515; NAIC § 9); and (5) the right to revoke authorization to use or disclose protected health information (HHS § 164.508(e); NAIC § 10).

C. *Differences*

Even though the NAIC Model Act and the proposed regulation have quite a few similarities, there are significant differences that concern the state insurance departments and the NAIC. As we witnessed in the legislative proposals offered by

[1] The "Health Information Privacy Model Act" and the "Insurance Information and Privacy Protection Model Act."

Congress, the smallest details can have a huge impact on how the privacy standards effect consumers and the states. Key differences are in scope and in the applicable entities impacted by the regulation.

HHS has expressed concern that because of its limited jurisdiction, the proposed regulation only applies to electronic health information and only applies to certain entities (64 Fed. Reg. 59923). We too are concerned about the limited reach of the proposed regulation.

1. *Scope* ("Summary and Purpose")

Both the NAIC Model Act and the proposed regulation establish standards to protect the privacy of protected health information. However, the proposed regulation defines protected health information to include only individually identifiable health information that is or has been transmitted electronically (HHS § 164.504). The regulation does not cover paper records. On the other hand, the NAIC Model Act does not distinguish between health information in paper format and health information that is electronically transmitted and maintained. The NAIC Model Act protects all forms of individually identifiable health information, both paper and electronic. We believe the NAIC Model Act's broader scope serves to better protect individuals' health information. (NAIC § 4).

HHS requested comment on whether it has the authority to extend protections to paper as well as electronic information, although to this point, HHS has limited its regulations to electronic information. (64 Fed. Reg. 59927). We suggest that since HHS believes it has the authority under HIPAA to extend these regulatory requirements to paper and electronic records, it should do so. Rather than wait to publish proposed rules that will govern paper records in the near future, we suggest that HHS address paper records in this current proposed regulation. The protections established in the proposed regulation should extend to both paper and electronic information.

2. *Applicable Entities* ("Applicability")

One of the most obvious differences between the NAIC Model Act and the proposed regulation is in the scope of the entities to which the respective proposals would apply. The NAIC Model Act only applies to insurance carriers. The proposed regulation is broader and applies to health plans, health care clearinghouses, and health care providers who transmit health information electronically. (HHS § 160.102). These entities are referred to in the proposed regulation as "covered entities." (HHS § 160.103).

Although the proposed regulation generally applies to a broader range of entities than the NAIC Model Act, we are concerned that "health plan" is defined in the proposed regulation to exclude certain insurers. The proposed regulation clarifies the definition of "health plan" established under HIPAA to include a health insurance issuer, a health maintenance organization, a Medicare supplement policy, and a long term care policy. (HHS § 160.103) As such, the proposed regulation would not apply to certain types of insurance entities, even if they provide coverage for health care services or use information found in an individual's medical record (i.e., life insurers, workers' compensation insurers, automobile insurers, other property-casualty insurers, and insurers offering certain limited benefits) (64 Fed. Reg. 59923, 59932). The NAIC Model Act applies to all insurers, regardless of the products that they sell.

While we recognize the limited jurisdiction of HHS under HIPAA with respect to insurers, we recommend the approach of the NAIC Model Act, which applies to all insurance carriers and is not limited to health insurers. (NAIC § 4). The NAIC had an extensive public discussion about whether the NAIC Model Act should apply only to health insurance carriers, or instead, to all carriers. Health insurance carriers are not the only types of carriers that use health information to transact their business. Health information is often essential to life insurers in issuing policies and to property and casualty insurers in settling workers' compensation claims and automobile claims involving personal injury, for example. Reinsurers also use protected health information to write reinsurance. The NAIC concluded that it was illogical to apply one set of rules to health insurance carriers but different rules, or no rules, to other carriers that were using the same type of information.[2] Consumers deserve the

[2] The NAIC Model Act does allow exceptions from the authorization requirement for certain insurers to conduct certain activities. These include: (a) when the protected health information is necessary to the performance of the carrier's obligations under any workers' compensation law or contract; and (b) when collecting protected health information from or disclosing protected health information to a reinsurer, stop loss or excess loss carrier for the purpose of underwrit-

Continued

same protection with respect to their health information, regardless of the entity using it. Nor is it equitable to subject health insurance carriers to more stringent rules than those applied to other insurers. Our model applies to all insurance carriers and establishes uniform rules to the greatest extent possible. The NAIC supports privacy protections that apply to individually identifiable health information wherever it resides.

II. Comments on Preemption ("Relationship to State Laws")

A. *General Comments on Preemption*

Preemption of state law is a key issue for the states and the NAIC membership. As we stated in our May 4, 1999 letter to Congress (Attachment B) and in Congressional testimony (Attachment C)[3], the federal government must recognize the impact of any privacy legislation or regulations on existing state laws. States have enacted many laws designed to protect an individual's health information in a variety of areas. These state protections appear in many locations within a state's statutes and regulations, and many times address programs or uses of health-related information that are unique to a particular state. In addition, states have carefully considered when to allow use and disclosure of health information without authorization, such as in cases of investigations and audits of health insurers by state insurance departments. States have enacted legislation and regulations after balancing the individual's right to keep health information confidential against the legitimate purposes for disclosure.

While we oppose the preemption of state law, we understand the desire to establish a minimum standard in this area due to several factors. First, the transmission of health information, as opposed to the delivery of health care services, is not always a local activity. Health information is transmitted across state and national boundaries. Second, while the NAIC has developed model legislation for the states to enact to protect individuals' health information that is collected, used and disclosed by insurance carriers, the reality is that our jurisdiction is limited to insurance. Because health information privacy encompasses more issues than insurance and more entities than insurers, we understand the desire for broader regulations. As a result, the members of the NAIC have concluded that the privacy of health information is an area where it may be appropriate for the federal government to set a minimum standard.

However, it should be noted that up until this point there has been no federal standard in place. Rather, states have been the protector of consumers in this area. Any federal action must recognize this fact and make allowances for it. The NAIC supports establishing a minimum federal level of protection for health information, as long as stronger state laws are preserved. We do not want to see health information that currently enjoys a high level of protection under state law end up with less protection under the proposed regulation.

For these reasons, we appreciate HHS' intent to create minimum standards, to preserve stronger state laws, and to protect certain state laws from any preemption. However, it is critical that the proposed regulation not undermine the progress of the states in implementing legislation that protects health information privacy and not undermine states' abilities to regulate entities over which they have jurisdiction. It is also critical that the proposed regulation, in its attempt to preserve state privacy laws, not make the process for states to enforce their laws so burdensome that the process only works in theory and not in reality.

B. *Preemption Standard in the Proposed Regulation*

In the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress directed HHS to implement privacy regulations if Congress failed to meet the statutory August 21, 1999 deadline to enact legislation. Congress also directed HHS to implement regulations that would not supercede a contrary provision of state law if the state law is more stringent than the regulation (HIPAA Sec. 264). While we appreciate the expressed intent of HHS in the preamble to preserve stronger state privacy laws and to protect other specific state privacy laws from preemption (64 Fed. Reg. 59994–59999), we have concerns about the language and structure used in the proposed regulation's general rule and the three categories of exceptions to

---

ing, claims adjudication and conducting claim file audits. However, these entities are subject to the rest of the model's provisions.

[3] Latest testimony dated July 20, 1999, before the House Ways and Means Committee, Subcommittee on Health is attached (Attachment C). The NAIC also testified two other times in 1999 on this issue: May 27, 1999 before the House Commerce Committee, Subcommittee on Health and the Environment; and April 27, 1999 before the Senate Health, Education, Labor and Pensions Committee.

the general rule. The preemption analysis used in the regulation is confusing and leaves many questions unanswered. Although the general rule and the exceptions were established in HIPAA by Congress, not by HHS, we believe HHS needs to make some clarifications in the proposed regulation in order to effectively and efficiently implement these standards.

C. *The Proposed Regulation's General Rule and Exceptions (HHS* § 160.203, 160.204)

1. *General Rule*

The NAIC membership has serious reservations about how the preemption standard used in the proposed regulation is to be implemented. The general rule established in HIPAA Section 262 and used in the current proposed regulation states that provisions of state law are preempted to the extent that they are contrary to the federal statutory and regulatory scheme. "Contrary" is defined in the proposed regulation such that: (1) complying with both state and federal requirements would be impossible; or (2) obeying state law prevents the accomplishment and execution of the full purposes and objectives of the regulation (HHS § 160.202). HHS has specifically requested comment on how these proposed criteria would be likely to operate with respect to particular state privacy laws (64 Fed. Reg. 59997).

While we recognize that HHS, in defining contrary, has used the standards developed by the courts for conflict preemption (64 Fed. Reg. 59997), we would note that in the past we have found similar definitions not to be very helpful in comparing state laws to federal requirements. We encounter a similar difficulty when conducting a conflict analysis for ERISA preemption using the "relates to" standard. Using the conflict analysis, a state must examine all its laws relating to health information privacy to determine whether or not its laws are contrary to the requirements in the proposed regulation. This in and of itself is a major project for states to undertake. Just identifying all of the laws, let alone comparing them to the federal regulation, is time-consuming and confusing for states. However, in response to HHS' request for comment, we offer a suggestion to help the operation of and to ease the administrative burden of implementing this standard.

We believe that how the term "provision" is defined will effect the practical implementation of the general rule. We propose that the states be given the greatest amount of flexibility in determining what the necessary scope of "provision" is when applying the general rule's contrary standard.[4] HHS has recognized that states know their laws best and are best informed about how to apply their laws. (64 Fed. Reg. 59998). The NAIC membership believes that the definition should preserve to the maximum extent possible state privacy initiatives that extend beyond the covered subject matter of the proposed regulation.

According to the preamble, when applying the general rule, what will be compared are state and federal requirements that are analogous, i.e., that address the same subject matter. If there is a state provision and no analogous provision in federal law, there is nothing to compare and no issue of a contrary requirement. (64 Fed. Reg. 59995). Consequently, if the state law is not contrary, the state law stands. If the state law is contrary, the state must go to the next step in the analysis to see if a contrary state law can still be saved from preemption by qualifying as one (or more) of the three categories of exemptions. We believe these are important statements and should be included as guidance in the regulation itself, not just in the preamble.

2. *Exceptions to Preemption of Contrary State Laws*

The exceptions to preemption for state laws that are contrary to the proposed regulation fall into three categories: (1) those state laws that require a determination by the Secretary that they are necessary for certain purposes as set out in HIPAA (HHS § 160.203(a); (2) those state laws that relate to the privacy of individually identifiable health information that are contrary to but more stringent than the federal requirements (HHS § 160.203(b)); and (3) those state laws that are explicitly carved out or exempted from the general rule of preemption (HHS § 160.203 (c), (d)).

These exceptions are established in the HIPAA statute, so we understand that HHS is prevented from adding or deleting any exceptions and is limited in how these exceptions are used. However, we have comments and concerns regarding each category of exceptions. Our most serious concerns lie with the exceptions that require a determination by the Secretary. We also seek clarification regarding how

[4] Our suggestion addresses HHS' request for comment on how the term "provision" might be defined (64 Fed. Reg. 59995).

these exceptions work on a practical level if a state law falls into more than one category of exception.

a. *Exceptions Requiring a Determination by the Secretary (Category One)*

Under this exception, a state may continue to enforce a contrary provision of state law that falls into one of five categories,[5] but only after obtaining a favorable determination from the Secretary of HHS. As set forth in the proposed regulation, if a state wants to continue to enforce a contrary provision of state law that falls under one of the listed categories, the state must submit a written request with detailed information to the Secretary seeking an exception to the preemption. Until the Secretary's determination is made, the federal requirement remains in effect. The Secretary will deny a request if it determines that the federal requirement accomplishes the law's purpose as well as or better than the state law for which the request is made. If an exception is granted, it is effective for three years or for such lesser time as is specified in the determination granting the request. (HHS § 160.204(a)).

We believe there are several serious flaws with this proposed process. Our primary concern is that the determination process is overly burdensome for states. Not only do states have to conduct a "contrary analysis" for all of their laws that protect health information and then submit requests for exceptions to HHS, but they also have to wait for HHS to make a determination in order for the states to enforce their laws.

We are very concerned about the provision in the proposed regulation that states that the federal standard applies until a determination is made (the statute is silent on this issue) (HHS § 160.204(a)(2)). This provision is unacceptable for insurance departments that are charged with protecting the citizens of the state and enforcing state laws regulating health plans. Cessation of state regulation in the interim will essentially leave plans unregulated until HHS makes a determination. The NAIC membership does not believe that the states should be hampered in their legal duties by having their laws preempted until they can prove to HHS that their laws are "necessary" for their states. States have passed privacy laws after careful consideration and debate, and they should not have to ask HHS for permission to enforce their own laws.

We offer a simple solution to this problem that would work within the confines of HIPAA and HHS' jurisdiction. The current assumption in the proposed regulation that the federal standard applies until a determination is made should be reversed. We believe there is enough latitude in the statute (i.e. the statute is silent) to reverse the presumption, so that a state law stands until and unless HHS has determined otherwise. The presumption should be in favor of the state's interpretation of its law. This reversal is necessary to avoid a regulatory vacuum, especially considering that the regulation does not establish a time frame within which the Secretary must make a decision. As a result, we believe state law should stand while HHS is making a determination.

On a related note, the NAIC membership questions whether HHS is prepared to conduct determinations for all 50 states' laws. After states complete their "contrary analysis," they will submit their state laws to HHS to make a determination. State privacy laws are found in many different areas of a state's statutes and regulations, so the Secretary may receive a number of requests per state. Without an increase in funding for HHS and the development of HHS' infrastructure, HHS will not be able to handle the volume of preemption determination requests from the states.

Another problem with the proposed regulation is the lack of details about the determination process. The proposed regulation does not establish a time frame or deadline by which HHS has to issue a determination. States could be waiting for years or indefinitely to find out whether HHS will grant an exemption. Such indecision could have a dampening effect on a state's ability to pass further legitimate legislation. We suggest that HHS revise its regulation to include a time period by which HHS has to make a determination. We also suggest that if HHS does not make a determination after a specified amount of time, then a default determination should be issued in favor of the state.

---

[5] The five categories are: (1) *the provision of state law is necessary to prevent fraud and abuse* (emphasis added); (2) *the provision of state law is necessary to ensure appropriate state regulation of insurance health plans* (emphasis added); (3) the provision of state law is necessary for state reporting on health care delivery or costs; (4) the provision of state law is necessary for other purposes related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system; and (5) the provision of state law addresses controlled substances. The italicized exceptions are of particular interest to the state insurance departments as the regulators of the insurance industry. (HHS § 160.203(a)).

We also are bothered by the fact that even if states are granted an exemption from preemption through the HHS determination process, there is a time limit on how long a state law is exempt pursuant to this determination (HHS § 160.203(a)(4). The process is quite burdensome for the states, so we question the provision requiring states to ask for a re-determination on the same laws every three years as a waste of time and resources for the states and for HHS. HHS should eliminate the three-year limit on how long the exemption is effective.

We are also concerned that there is no requirement in the regulation regarding giving notice to the states and others that HHS has made a determination, other than an annual publication in the Federal Register of all determinations made by HHS. (HHS §160.203(a)(8). More frequent notices, such as quarterly, should be made. We also suggest that HHS provide more details in the proposed regulation about the factors it will consider in its determination process and if there is a formula HHS will use to decide whether a state will be granted an exemption.

b. *Exception for State Laws that are More Stringent than the Regulation (Category Two)*

The second exception allows a state to continue to enforce a contrary provision of state law that relates to the privacy of health information if it is more stringent than a standard, requirement, or implementation specification adopted under the proposed regulation. More stringent is broadly defined in the proposed regulation as providing greater privacy protections for the individual. A state is not required to obtain a determination about whether a provision of its law meets this exception. However, the Secretary on her own, or at the request of a state, may issue an advisory opinion as to whether a provision of state law meets this exception. (HHS § 160.204(b)).

In the NAIC's Congressional testimony (see attached), we supported the establishment of minimum standards in the area of health information privacy, and we urged Congress to outline a way in its legislation for the states to measure their laws against any federal standard. We appreciate that HHS has chosen to establish minimum federal standards and has included guidelines for states to measure their laws against the proposed regulation (i.e., less disclosure to others; greater right of access to health information by the individual; greater penalties; narrower scope of authorization; longer record-keeping requirements and accounting requirements.). States need to be able to judge whether their state laws are stronger than any federal standard in order to determine whether they need to take further action to revise their laws. By defining "more stringent" in the proposed regulation, HHS has offered several different examples of what qualifies as more stringent as guidance to the states, with the overriding principle of more protection to the individual whose information is being used or disclosed. (HHS § 160.202).

Additionally, we support HHS' decision to limit the parties who may request advisory opinions to the states and the Secretary of HHS. (HHS § 160.204(b)(1); 64 Fed. Reg. 59998). We do not believe that insurers should be allowed to request an advisory opinion and open every state law up to challenge and to review by HHS.

We do have one concern regarding this exception that we believe could be resolved with explicit clarification. Since the federal regulation only applies to individually identifiable health information that is electronically maintained and transferred and it only applies to health insurers, not all insurers, we would like assurance that the NAIC Model Act and similar state laws, which have a much broader scope (apply to all forms of transmission and to all insurers), would be viewed as more stringent and would be allowed to stand under the proposed regulation. We believe that these broader state laws would fall under the category of "providing greater privacy protection for the individual," but explicit clarification in the preamble or text or even inclusion in the list of examples would be appreciated. The regulation should preserve state laws to the maximum extent possible and allow states to enforce their laws as they apply to entities and situations that are beyond the scope of the regulation.

Overall, we are supportive of this exception and how HHS has addressed the issue in the regulation. This federal floor exception will still require the states to analyze their laws regarding whether the laws are contrary and more stringent than the proposed regulation. However, the states will not have to go through the burdensome process as required by the category one exceptions, and they will not be prevented from enforcing their laws waiting for a determination. In addition, this exception allows states to enact stronger laws where and when they are needed and to enact laws in the future to address changes in technology and in the use of health information and to address state-specific issues.

c. *Exceptions that are State Law Carve-Outs (Category Three)*

Under the third category of exceptions, a state may continue to enforce a contrary provision of state law that the meets one of the two specified exceptions: (1) provisions of state law requiring the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention; and (2) *provisions of state law requiring a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, facility licensure or certification,* or individual licensure or certification (emphasis added). (HHS § 160.203(c), (d)). No mechanism is required or available under the proposed regulation for determining whether a state law meets one of these complete carve out exceptions. It appears to be left up to the discretion of the states, although the NAIC membership requests that HHS affirmatively state this fact.

The second carve out above is of interest to us. Although state insurance laws would qualify for this exception, we are concerned with the scope of the exemption regarding oversight of health plans. We realize this list of activities related to state insurance department oversight is set forth in HIPAA § 262 (Social Security Act § 1178); however, the preamble of the proposed regulation explains that § 1178 carves out an area which the states traditionally have regulated and which the statute intends to preserve for the states (64 Fed. Reg. 59999). We are concerned because the list has omitted some very important activities that are traditionally regulated by the states in the area of health care, specifically such activities as market conduct examinations, enforcement investigations or consumer complaint handling. While it is possible that these functions may be included within other categories that are itemized, it is certainly not clear that these functions would fall within the exemption. The NAIC membership thinks that the proposed regulation should recognize that these and other state insurance department activities are covered under this exception. The stated intent is to preserve an area of law traditionally regulated by the states, therefore we request that the regulation clarify, either in the preamble or the text, that a broad scope of state insurance department activities fall within this carve out.

3. *Interaction Among the Three Categories of Exceptions*

We request a clarification regarding state laws that are contrary to the proposed regulation but that could fall into more than one category of exception. Clearly the proposed regulation contemplates a state law falling into more than one exception (HHS § 160.203), especially since the three categories of exceptions are drawn broadly. We believe state insurance laws easily could fall into several categories of exceptions. An example is state laws regulating health insurance plans (category one) that are more stringent than the federal regulation (category two) and require health insurance plans to report information (category 3). However, this language raises several questions: (1) If a state law falls into more than one exception, do states get to choose which category of exception applies? (2) Will insurers, consumers or others be allowed to sue state insurance departments if they do not agree with the departments' classifications of the laws? (3) Will this issue result in litigation in order to resolve which category of exception any particular state law falls into? We think a simple clarification statement in the regulation will answer these questions.

We ask HHS to include language in the text of the proposed regulation stating that if a state law falls within several different exceptions, the state chooses which exception shall apply. Clearly, the states would prefer a category three exception (complete carve-out) over a category two exception (optional advisory opinion), and a category two exception over a category one exception (required prior determination). The presumption should be that the state has the best knowledge of its laws and it has correctly classified its laws in the appropriate category of exceptions. HHS even recognized in the preamble that states are the most knowledgeable about their own laws. (64 Fed. Reg. 59998). We think this simple clarification statement will avert much litigation and prevent state insurance departments from having to defend endless challenges to their classification of their laws.

III. Comments on Exceptions from the Authorization Requirement for Disclosure to Health Oversight Agencies for Health Oversight Activities (HHS § 164.510(c)); *for Disclosure for Law Enforcement Purposes (HHS* § 164.510(f)); *and for Use and Disclosure for Judicial and Administrative Proceedings (HHS* § 164.510(d)). *("Health Oversight," "Law Enforcement," and "Judicial and Administrative Proceedings")*

A. *Classification of State Insurance Departments*

Similar to the NAIC Model Act, the proposed regulation establishes a list of exceptions to the authorization requirement, such that protected health information

may be used or disclosed without authorization in certain circumstances. However, under the HHS proposed regulation, the activities of state insurance departments fit under any one or more of the following three exceptions: (1) for disclosure to health oversight agencies for health oversight activities; (2) for disclosure for law enforcement purposes; and (3) for use and disclosure for judicial and administrative proceedings. The regulation is unclear about the role of insurance departments relative to these exceptions.

1. *Health Oversight Agencies and Their Activities (HHS* § 164.510(c))

The definition of "health oversight agency"[6] most clearly encompasses and applies to state insurance departments. Although the preamble specifically lists state insurance departments as included in this category, we suggest including this statement in the text of the regulation, not just the preamble (64 Fed. Reg. 59958).

The proposed regulation provides an exception to the authorization requirement for disclosure to health oversight agencies for conducting health oversight activities. According to the proposed regulation, these health oversight activities authorized by law include audits; investigations; inspections; civil, criminal or administrative proceedings or actions; and other activities necessary for appropriate oversight of: i) the health care system; ii) government benefit programs for which health information is relevant to beneficiary eligibility; or iii) government regulatory programs for which health information is necessary for determining compliance with program standards (HHS § 164.510(c)(1)).

We are particularly concerned about the scope of the exemption in terms of the listed activities that are included for state oversight of health plans. While the list includes a large catch-all category for "other activities necessary for appropriate oversight of the health care system, government benefit programs, or of government regulatory programs," the list fails to include other oversight activities that are of such importance to state insurance departments that they should be specifically listed. Some of these oversight activities that are traditionally conducted by the states are: market conduct examinations; consumer complaint handling; solvency and financial examinations; rehabilitation and liquidation; investigations; audits; fraud activities; establishing and enforcing legal or fiscal standards relating to the regulation of the business of insurance, including claims, underwriting, sales, and managed care; assessments, evaluations, determinations; initiation of administrative, civil or criminal proceedings; compliance and enforcement of laws or regulations.

While it could be argued that some of these functions are included within other categories that are itemized, it is certainly not clear that these functions would fall within the exemption. In order to ensure that every insurance department can fulfill its obligations to the citizens in its state, we request that HHS add these additional oversight activities to the list of specific examples. We also request that HHS clarify that the catch-all exemption to the authorization requirement for activities necessary for the appropriate oversight of the health care system is intended to include all legally authorized activities performed by insurance departments.

2. *Health Oversight Activities by Two or More Agencies.*

On a related note, the preamble states that in cases where health oversight agencies are working in tandem with other agencies overseeing public benefit programs to address compliance, fraud or other integrity issues that could span across programs, the oversight activities of the team would be considered health oversight and disclosure to and among team members would be permitted under the proposed rule to the extent permitted under other law. (64 Fed. Reg. 59958). We appreciate that state agencies will be able to work together and share protected health information among agencies in order to conduct oversight activities and share information, without being considered as business partners or needing a contract to share information among state agencies.

However, we would like to see this ability to share information with other agencies for oversight purposes expanded from just overseeing public benefit programs (i.e. Medicaid) to overseeing health programs and activities as a whole. For example, an insurance department may not be the sole agency in a state that regulates health insurers and plans. In some states, the Department of Health, the Department of Corporations or the Department of Managed Care is responsible for regulating managed care entities. This results in an overlap in jurisdiction or in delegation

[6] "Health oversight agency" is defined as an agency, person or entity, including the employees or agents, that is a public agency (or acting under a grant of authority from or contract with a public agency) and which performs or oversees the performance of any audit; investigation; inspection; licensure or discipline; civil or criminal or administrative proceeding or action; or other activity necessary for appropriate oversight the health care system. (HHS § 164.504).

of responsibilities among agencies for regulating the health insurance entities. Sharing of information among agencies for these oversight activities is just as important as oversight of public benefit programs. Consequently, we would like to see the regulation recognize the need for information-sharing among agencies for the oversight of health programs and activities as a whole.

3. *Law Enforcement and Judicial and Administrative Proceedings (HHS* § 164.510(f), (d))

In addition to falling into the health oversight exception, it could be argued that certain state insurance department activities fall under the law enforcement and judicial and administrative proceeding exceptions. The definition of "law enforcement official" is very broad and includes an officer of an agency or authority of a state who is empowered by law to conduct: 1) an investigation into a violation of, or failure to comply with any law; or 2) a criminal, civil or administrative proceeding arising from a violation of, or failure to comply with, any law. (HHS § 164.510(f)(1)(ii); 64 Fed. Reg. 59937). Because of their job responsibilities, state insurance commissioners would fall into this definition. As drafted, state insurance department efforts to combat health care fraud could be considered law enforcement activity.

Judicial and administrative proceedings are not defined in the proposed regulation but are considered an exception to the authorization requirement. Under this exception, persons are permitted to disclose information in the course of any judicial or administrative proceeding, but only in response to an order of a court or administrative tribunal, or where the individual is a party to the proceeding and his or her medical condition or history is at issue and the disclosure is pursuant to lawful process or otherwise authorized by law. (HHS § 164.510(d)(1)). State insurance departments conduct administrative proceedings and are often involved in judicial and administrative proceedings.

Potentially, one single activity could be construed as falling into all three exceptions. An example could be a joint investigation by an insurance department's investigation team, which is investigating a licensee for purposes of determine if administrative action should be taken against the licensee, and the department's fraud unit, which may prosecute the individual for insurance fraud. This issue raises procedural questions, especially if one exception requires a court order (judicial and administrative proceedings), one does not (health care oversight), and another exception may require a court order in certain situations (law enforcement, although not for health care fraud). The preamble states that agencies that conduct both oversight and law enforcement activities would be subject to the provision on use and disclosure for health oversight activities when conducting oversight activities (64 Fed. Reg. 59958). However, what standards apply when conducting other activities. It is difficult to have several different applicable rules based on the activities the states are performing. This is especially true if states are conducting activities that fall into more than one category of exception and the activities are not so easily divided into parts that need authorization and those that do not.

The regulation should state that either insurance departments decide which exception applies, or that all insurance department activities are health oversight activities. Otherwise, state insurance departments may face endless litigation over their classifications. We ask HHS to include language in the text of the proposed regulation stating that if a state insurance activity falls within several different exceptions, the state chooses which exception shall apply. The presumption should be that the state has the best knowledge of its laws and activities and has correctly classified them in the appropriate category of exceptions. HHS even recognized in the preamble that states are the most knowledgeable about their own laws (64 Fed. Reg. 59998). We think this simple clarification statement will avert much litigation and prevent a state insurance department from having to defend endless challenges to its classification of the exception that applies.

B. *Permitted Disclosures Versus Required Disclosures to State Insurance Departments*

We are concerned that under the proposed regulation covered entities are "permitted" but not "required" to disclose necessary protected health information to health oversight and law enforcement agencies (HHS § 164.510(c), (f); 64 Fed. Reg. 59955). Under the proposed regulation, disclosure is required in only two instances—to permit an individual to inspect or copy their information, or when required by the Secretary. (HHS § 164.506)

We believe that covered entities under investigation by a state agency should be required to provide that state agency with access to necessary health information when performing its legally mandated duties. This disclosure should not be optional. By not requiring insurers to provide state insurance departments with access to

records, filings and other documents that may contain individually identifiable information, state insurance departments' ability and authority to perform their regulatory responsibilities is undermined. In addition, obtaining authorization from all of an insurer's clients for investigation of an insurer's business practices is not feasible or practical.

The NAIC requests that disclosure be required under the proposed regulation in additional instances, including disclosure to health oversight agencies for health oversight activities consistent with state law. The NAIC Model Act lists circumstances where an insurer is required to disclose protected health information without an authorization. Three of these situations are: (1) disclosure to federal, state or local authorities to the extent the carrier is required by law to report protected health information or for fraud reporting purposes; (2) disclosure to a state insurance department performing an examination, investigation, audit; or (3) pursuant to a court order. (NAIC Model Act § 11). By not requiring insurers to disclose needed records that may contain individually identifiable health information, state insurance departments will be forced to obtain court orders for every request of information needed for a legitimate and lawful purpose.

However, even court orders will not remedy the problem, since under the proposed regulation's judicial and administrative proceeding exception, covered entities are permitted to disclose protected health information in a judicial or administrative proceeding if the request for such protected health information is made through or pursuant to an order by the court or administrative tribunal. (HHS § 164.510(d)). This use of "permitted" in the proposed regulation instead of "required" will severely hamper state insurance departments from doing their jobs.

The preamble states that protected health information is often needed as part of an administrative or judicial proceeding, and it even lists examples. The preamble states that these "uses of health information are clearly necessary to allow the smooth functioning of the legal system." (64 Fed. Reg. 59958–59959). If the uses are necessary, it logically follows that the language in the text of the proposed regulation should use the word "required" instead of "permitted."

IV. Comments on Accounting for Disclosures Requirement (HHS § 164.515)

Both the proposed regulation and the NAIC Model Act grant individuals the right to an accounting of the disclosures of their protected health information from covered entities (HHS § 164.515; NAIC § 9), and both establish exceptions to this right. The proposed regulation establishes an exception so that accounting for disclosure to an oversight agency or law enforcement agency is not required to be given to an individual if the agency provides a written request stating that the exclusion is necessary for a specified period of time. (HHS § 164.515(a)(2)). The NAIC Model Act's exception states that the carrier is not required to include in the accounting any disclosures of protected health information that were compiled in preparation for litigation, law enforcement or fraud investigation. There is no date-specific deadline on this exception.

Both the proposed regulation and the NAIC Model Act create exceptions to the accounting requirement for oversight agencies and law enforcement agencies conducting investigations. The problem with the proposed regulation is that it is nearly impossible to accurately project the length of an investigation, especially during its early stages. Rather than designating a specific date or a specific amount of time for no accounting of disclosures to oversight or law enforcement agencies, the NAIC suggests a deadline based on the end of an event, such as conclusion of an investigation. This ensures that an individual will receive a full accounting of disclosures at a certain point but also allows an oversight or law enforcement agency to complete its investigation without having to set some arbitrary date of disclosure.

V. Comments on Banking Activities and Financial Services Modernization (HHS § 164.510(i)) ("Banking and Payment Processes")

HHS attempts to address banks and banking activities within the scope of the proposed regulation. We believe this is a very important issue in light of the passage of financial services modernization legislation, The Gramm-Leach-Bliley Act, Public Law 106–102 (the "GLB Act"), and with the changes in the entities that are considered "payers." However, we have some concerns about how banks and their activities are handled under the proposed regulation.

A. *Payment Activities Versus Non-Payment Activities*

The first issue concerns the exception for banking and payment processes (HHS § 164.510(i)). This exception is confusing because HHS attempts to address two separate issues within the context of this one exception—payment activities and non-payment banking activities. We believe these two issues should be handled separately.

Under the statute (§ 1179 of the Social Security Act/§ 262 of HIPAA), banks can use or disclose protected health information for certain listed purposes (all involving payment), and HHS repeats these approved activities in the regulation.[7] billing, transferring, reconciling or collecting payments'' for health care or health plan premiums.

Under § 164.510(i), ''disclosure for banking and payment processes,'' covered entities are allowed to disclose protected health information to financial institutions without an individual's authorization for processing payment for health care and health care premiums, including the processing of checks or credit card transactions as payment for health care services.[8] However, covered entities would not be allowed under the proposed regulation to include any diagnostic or treatment information in the data transmitted to financial institutions. (64 Fed. Reg. 59966).

We agree with HHS' assessment of a bank's role in payment activities. We too recognize that a certain amount of information is needed to process payments, but we agree that a bank would not need diagnostic or treatment information in order to process a payment and that in most cases, if not all, only the specified information would be necessary for a bank to conduct payment activities.[9] (64 Fed. Reg. 59966).

HHS also raises the issue of non-payment banking activities in the preamble of this exception (not in the text of the proposed regulation). HHS theorizes about activities banks may be providing now and in the future for plans and providers, and HHS recognizes that banks, in addition to offering traditional banking services, may be interested in offering additional services to covered entities such as tracking services, and diagnostic and treatment information, claims management and billing support. (64 Fed. Reg. 59966). With the passage of the GLB Act, this is a very real scenario.

Currently, banks are not considered covered entities under this proposed regulation. HHS tries to address its lack of jurisdiction over banks by classifying banks as ''business partners'' of covered entities when receiving protected health information for non-payment activities.[10] (64 Fed. Reg. 59966). For example, if a bank offers an integrated package of traditional banking services and health claims and billing services, it could do so through a business partner arrangement that meets the proposed requirements. (64 Fed. Reg. 59966–59967).

We agree with HHS' assessment that nothing in the regulation would prohibit banks from becoming business partners of covered entities under the conditions established in the proposed regulation (HHS § 164.506(e)), and that any services offered by a bank that are not on the list of exempt services in the statute (Social Security Act § 1179) should be subject to the business partner rule. We also agree that disclosing protected health information to a financial institution for non-payment activities without authorization or without a business partner contract would violate the provisions of the proposed regulation. (64 Fed. Reg. 59966).

As demonstrated by our comments, our concerns do not involve how HHS has addressed payment activities or non-payment activities of banks, but rather that HHS has addressed these two issues together as if there were no differences in the need for protected health information in these two sets of activities. We think that bank activities that do not involve processing payments should be handled separately from payment activities. The exception (HHS § 164.510(i)) should be narrowed to be just ''payment processes'' and should not be ''payment and banking processes'' or

---

[7] These activities are ''authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting payments'' for health care or health plan premiums.

[8] We question the need for the exception for disclosure for banking and payment processes. Under the general rule, authorization is not required for payment purposes. Presumably a covered entity would not need an authorization to disclose protected health information to a bank for payment purposes. However, one of the additional listed exceptions is for disclosure for banking and payment processes. This exception appears to be duplicative of the general rule, which raises the question of why this is an exception. It appears HHS wants to limit the amount of information that a bank can receive to process a payment, specifically a check or a credit card transaction. This is less of an exception to the general rule and more of a clarification of the rule, since the rule already excepts payment activities.

[9] Limited list would include only: (1) the name and address of the account holder; (2) the name and address of the payer or provider; (3) the amount of the charge for health services; (4) the date on which health services were rendered; (5) the expiration date for the payment mechanism, if applicable (i.e., credit card expiration date); and (6) the individual's signature.

[10] A covered entity may disclose protected health information to persons it hires to perform functions on its behalf (''business partners''), where such information is needed for that function. However, a covered entity and its business partners would be required to enter into a contract that establish the permitted and required uses and disclosures of such information by the partners.

any other activities outside the scope of payment. All other non-payment activities should be governed by the business partners rule.

In addition, there are discrepancies between the preamble and the actual text of the regulation setting forth this exception (HHS § 164.510(i)). Notwithstanding the discussion on banks as business partners, the intent of the preamble seems fairly focused and is narrower in scope than the actual text. The text of the regulation as it is currently written is overly broad and could lead to unintended consequences. The preamble addresses payment processes, but the text of the regulation addresses "routine banking activities or payment." (64 Fed. Reg. 59966; § 164.510(i). "Routine banking activities" is very broad and could include approving loans and offering mortgages—activities that do not necessitate disclosure of protected health information for payment, but would be allowed under the text of the regulation. Banks should not have access to individuals' protected health information in deciding whether to offer a loan or mortgage. We suggest that the text of the regulation be re-drafted to reflect the narrower scope and intent of the preamble.

In short, if covered entities disclose protected health information to banks strictly for payment processing, we agree that no authorization is needed, but the information banks receive should be minimal. If protected health information is used for any other reason, authorization from the individual would be required or a business contract with a covered entity would be required.

B. *Banks as "Covered Entities"*

Currently banks are not included under the definition of "covered entities" in the HHS proposed regulation; however, with the enactment of the GLB Act, banks are able to form holding companies that will include insurance companies (covered entities) and their activities.[11] As a result, banks may soon have access to protected health information once the GLB Act is implemented and banks start buying insurance companies. When (not if) this happens, we believe banks should be classified as covered entities under the proposed regulation. Banks should be held to the requirements of the HHS proposed regulation and should be required to obtain authorization from an individual to conduct non-payment activities. As listed in the preamble, these activities requiring authorization would include: use for marketing of health and non-health items and services; and use and disclosure to non-health related divisions of the covered entity (e.g., for use in marketing life or casualty insurance or banking services). (64 Fed. Reg. 59941–59942). HHS should clarify that if financial institutions act as payers, they should be governed by the HHS privacy regulation as covered entities.

VI. *Conclusion*

In summary, we support HHS' efforts to implement privacy regulations that leave intact as many state laws as possible. However, we do have serious concerns about the scope, the applicable entities effected by the proposed regulation, the preemption of state law, the determination process for preemption exceptions, and how state insurance departments and the broad scope of activities for which they are responsible are classified. We believe that the regulation in its current form has the potential to significantly impair the states' ability to regulate the health insurance industry. We do believe that the proposed regulation may be workable if HHS implements our suggested changes.

The NAIC appreciates the opportunity to offer these comments regarding the proposed regulation. The NAIC intends to continue working closely with HHS on these and other issues. If HHS has any questions with respect to these comments or any

---

[11] We are concerned about the relationship between the GLB Act and its proposed privacy regulations and HHS' proposed health information privacy regulation. Under the GLB Act, a bank holding company has affiliates that may be insurance companies, securities firms, or thrifts. These affiliates are allowed to exchange personally identifiable financial information with each other and with the bank holding company without authorization from the individual. The only restrictions on sharing this information under the GLB Act is with non-affiliated third parties. Under the HHS proposed regulation, an insurance company could not share protected health information with an affiliate without a business partner contract. Clearly, the GLB Act is less restrictive in the use and disclosure of protected health information and is less protective of individuals' rights than the HHS proposed regulation.

Consideration needs to be given to the interaction between the HHS proposed privacy regulation, the financial services modernization legislation and proposed regulations, and state laws. In addition to the impact on state laws, we are concerned about the interaction and potential conflict between the two federal laws and their regulations. In general, the relationship between the preemption standards of HIPAA and the GLB Act, as they relate to financial institutions, is not clear and is still being analyzed and interpreted by many interested parties including the NAIC. We ask that HHS work with the federal agencies (Federal Reserve, Treasury, Office Thrift Supervision, etc.) that are involved in promulgating regulations to implement the GLB Act to discuss the potential conflicts between the competing privacy regulations.

other element of the proposed regulation, it should feel free to contact myself or Mary Beth Senkewicz at (202) 624–7790.

Sincerely,

KATHLEEN SEBELIUS
Vice President,
Chair, Health Insurance Task Force
Commissioner of Insurance, Kansas

Attachments
National Association of Insurance Commissioners
Federal and International Relations Office
Hall of the States
444 N. Capitol Street, N.W.
Suite 701
Washington, D.C. 20001
(202) 624–7790

NATIONAL BREAST CANCER COALITION
WASHINGTON, DC 20036
February 15, 2000

U.S. Department of Health and Human Services
Assistant Secretary for Planning and Evaluation
Attention: Privacy-P, Room G–322A
Hubert Humphrey Building
200 Independence Avenue, SW
Washington, D.C. 20201

Dear Assistant Secretary for Planning and Evaluation:

I am writing to you on behalf of the National Breast Cancer Coalition (NBCC), and the 2.6 million women living with breast cancer. NBCC, a grassroots advocacy organization made up of over 500 organizations and tens of thousands of individuals, has been working since l99l to eradicate breast cancer through increased funding and new strategies for breast cancer research, access to quality health care for all women, and expanded influence of breast cancer activists at every table where decisions regarding breast cancer are made.

NBCC strongly believes that we must establish a national policy that ensures an individual's right to privacy with respect to individually identifiable health information. Individuals own their health information. The issue here is under what circumstances other people should be able to use an individual's health information. As breast cancer survivors, we believe that our illness, diagnosis, treatment and prognosis is very personal information. We also know that the misuse of our health information can harm us and our families. For example, unauthorized or inadvertent disclosure of our health status, genetic or family history can make it difficult if not impossible for some women and their daughters to obtain health insurance. This danger becomes an increasing reality as the number of entities maintaining and transmitting individually identifiable health information and the use of integrated health information systems generally continues to grow. Without any national privacy standards to protect consumer's rights, consumers risk misuse of health information within an uneven system of state protection.

At the same time, NBCC believes that federal standards for protecting privacy rights should not impede the progress of biomedical, behavioral, epidemiological and health services research. Research offers women diagnosed with breast cancer the best hope for finding a cure and improving treatment, and someday preventing breast cancer. NBCC believes that a federal standard should protect the privacy of individuals and enhance public trust in medical research, and simultaneously protect the ability of researchers to conduct vital biomedical research.

The following comments are in response to the Department of Health and Human Services' (HHS) proposed rule (45 CFR Parts 160 through 164). NBCC commends HHS for developing significant regulatory standards that aim to fill the gap in federal health privacy protection. While the draft regulations properly address several of NBCC's key concerns—such as access to medical records; notice of information policies; informed consent; minimum necessary use; and the use and disclosure of personal health information with regard to research—we remain concerned about the areas that HHS did not have the authority to cover. It is for that reason that we continue to urge Congress to enact comprehensive federal privacy legislation.

We appreciate the opportunity to comment on the health privacy regulations, and look forward to working with HHS and Congress to improve health information privacy.

The Regulations are not sufficiently broad in scope.

1. The Regulations cover a limited number of entities. (Section 164.502)

NBCC recognizes that HIPPA specifically limited the entities that HHS could cover—so that the regulations could only apply to health plans, health care providers and health care clearinghouses. These three categories exclude a number of entities that receive health information, such as contractors, third party-administrators, researchers, public health officials, life insurance insurers, employers and marketing firms. The regulation's limited coverage of entities is a serious flaw. Congress must continue to work towards enacting a comprehensive federal privacy law that would apply to all of those who generate, maintain or receive protected health information.

2. The Regulations only cover protected health information that is electronically transmitted. (Section 164.504)

Another limitation of the draft regulations is that they only apply to "protected health information" which is defined as individually identifiable health information that has been transmitted or maintained *electronically* by a covered entity. This means that all private health information that remains in *paper form* would be unprotected.

Privacy standards must apply to all individually identifiable health information in *any* form maintained or transmitted by a covered entity. It does not make any sense to draw a distinction based on form rather than content. A covered entity should be required to treat all information it maintains or transmits in the same fashion. Covered entities currently maintain and transmit health information in both electronic *and* paper form. In fact, many health care providers maintain solely paper systems and a majority of health information remains in paper form. If the regulations do not apply to this information in any form, they will not accomplish the goal of protecting individuals' medical privacy. People or organizations that hold health information that would otherwise be protected could escape compliance with privacy protections by maintaining the records on paper. Additionally, for enforcement purposes, it may prove difficult, if not impossible, to establish that specific health information at some point in its existence has been transmitted or maintained electronically and, therefore, is subject to the regulations. The best way to reduce these implementation and enforcement ambiguities is to make the privacy standards applicable to all individually identifiable health information transmitted or maintained by a covered entity regardless of its form.

3. The Regulations should explicitly include genetic information in the definition of individually identifiable health information. (Section 164.504)

NBCC strongly believes that the definition of individually identifiable health information is also flawed. While "individually identifiable health information" is defined as information that "relates to the past, present or future physical or mental health or condition of an individual," this definition does not explicitly include genetic information. NBCC urges the Secretary to amend the definition of individually identifiable health information so that genetic information is afforded the same protection as other medical information.

Individuals must have rights
regarding their health information.

1. Individuals must have the right to access, amend and correct protected health information. (Sections 164.514, 164.516)

NBCC strongly believes that individuals should have certain rights with regard to their medical records and information in order to understand how they are being used and maintained. Individuals should have reasonable access to their records to inspect, copy, supplement or amend their medical records so that they can make informed health care decisions and correct errors where appropriate. The regulations appropriately provide for these individual rights. Any exceptions that would deny an individual's access must be extremely limited and narrowly construed.

2. Individuals must have the right to restrict uses and disclosures of their health information. (Section 164.506(c))

NBCC also believes that individuals should have the right to restrict a covered entity from continuing to use and disclose protected health information. Patients have legitimate concerns that ongoing disclosures could result in personal harm or discrimination. Individuals should be able to seek special protection for certain sensitive information that they do not wish to be disclosed. For example, many women may wish to prevent a health care provider from disclosing BRCA1 and BRCA2 test results. Accordingly, NBCC supports the general idea behind the regulations' granting individuals the right to request restrictions on the uses and disclosures of protected health information. However, the regulations must provide stronger protections by binding all covered entities to any restriction requested by an individual (except in emergency situations or when it would harm the individual) and requiring them to comply or face consequences.

Individuals must be given notice of information practices. (Sections 164.512, 164.520)

It is important that individuals understand how their medical records are to be used and when and under what circumstances that information will be disclosed to a third party. Individuals should be given easy-to-understand written notice of how their health information will be used and by whom. Only with such notice can people make informed, meaningful choices about uses and disclosures of their health information. Adequate notice can also help to build trust between patients and health care provider organizations in so far as it removes any element of surprise about the use and disclosure of health information. NBCC believes that the proposed regulation properly gives individuals the right to adequate notice of the disclosure policies of covered plans and providers.

Individuals' informed consent should be obtained in most instances.

1. Informed consent must be obtained for uses and disclosures unrelated to health care. (Section 164.508)

NBCC believes that a covered entity must obtain an individual's specific authorization if it intends to use or disclose protected health information for any purpose other than treatment, payment or health care operations. Consumers regularly sign a general authorization that allows providers and plans to use their personal health information for treatment, payment or health care operations. However, there are many other uses that they might not anticipate and would want to know about. For example, breast cancer patients do not expect that information concerning their individual treatment will be released for targeted marketing of new products based on their health status. Nor would they necessarily want non-health related divisions of an employer who provides health insurance to obtain protected health information for eligibility or enrollment determinations, underwriting risk determinations, or employment determinations. Another unforeseen use is research unrelated to health care, for which there is insufficient scientific and medical evidence regarding the validity or utility of the information. Such research might utilize their health information to discover genetic markers that could later be used to discriminate against women with a genetic predisposition for breast cancer. For uses such as these that are not directly related to treatment, payment, or health care operations, NBCC encourages the Secretary to retain provisions of the proposed regulations that require covered entities to obtain separate and specific authorization from individuals.

Requiring individuals' explicit authorization for these uses would enhance individuals' control over their protected health information, if and only if, the authorizations are specific about the information to be disclosed and where the information will go. Furthermore, in order for individuals to voluntarily authorize such disclosures, their authorization must not be coerced, as a condition of payment. NBCC suggests that the regulations be revised to expressly provide that a covered entity and its business partners may use or disclose protected health information only for the purpose specified in the authorization. This would help ensure that the information does not fall into the hands of non-covered entities that are not subject to the protections afforded by the regulations.

2. Circumstances under which informed consent is not required should be strictly limited.

Federal privacy standards should strictly limit the circumstances under which individuals' identifiable health information can be used without their informed consent. The Secretary has proposed that covered entities could use and disclose protected health information without authorization for: (1) treatment, payment, and health care operations; and (2) national priority activities.

(a) Informed consent is not necessary for uses and disclosures related to treatment, payment and health care operations if the meaning of these terms is narrowly interpreted. (Section 164.506)

Uses and disclosures related to treatment, payment and health care operations include purposes such as quality assurance, utilization review, credentialing, and other activities that are part of ensuring appropriate treatment and payment. While NBCC generally agrees that informed consent is not necessary for these purposes, the provisions addressing the meaning of treatment, payment, and health care operations should be amended. For example, the terms "treatment" and "payment" should be narrowly interpreted as applying to the individual who is the subject of the information. In addition, the definition of "treatment" should be amended to ensure that disease management programs are only conducted with the authorization of the treating physician. The regulation should also expressly state that the term "health care operations" includes only disclosures made to the covered entity (or a business partner of such entity) on whose behalf the operation is being performed. Furthermore, the regulations should limit the definition of health care operations to include only those operations that cannot be carried on with reasonable effectiveness and efficiency without protected health information.

(b) Generally, informed consent is not necessary for uses and disclosures related to national priority activities. (Section 164.510 (b) through (n)

The regulations also provide that individually identifiable information could be disclosed without informed consent for the following national priority activities: health care oversight, public health, emergency purposes, research, judicial and administrative proceedings, law enforcement, and to provide information to next-of-kin. While NBCC notes the importance of these activities, we urge that the final regulation include certain safeguards to protect individuals against arbitrary disclosures for law enforcement purposes.

Law enforcement should not have unfettered access to medical records. (Section 164.510(f))

We believe that the federal law protecting the privacy of health information should be just as strong, if not stronger, than the protections for cable and video records. Medical records contain personal and sensitive information, and the misuse of peoples' medical information can lead to loss of jobs and benefits, discrimination, embarrassment, and other harms. However, under the regulations, medical records are not afforded the same protections with regard to disclosures for law enforcement purposes. In light of the importance of medical records, we recommend that law enforcement be required to obtain legal process—such as a warrant or court order—that is judicially-approved after application of a Fourth Amendment probable cause standard.

PRIVACY STANDARDS SHOULD NOT IMPEDEDE MEDICAL RESEARCH.

1. All research information related to health care should be reviewed under privacy standards before waiver of individual authorization can occur. (Section 164.510(j))

There has been much debate about what are appropriate safeguards for personally identifiable information with regard to research. Increasingly, health services, epidemiological, biological and statistical research utilizes medical or health records and does not involve any interaction between the researcher and the patients. Researchers have legitimately raised serious questions about the feasibility of seeking authorizations from thousands or possibly millions of individuals. Other research such as retrospective or secondary research also utilizes archival patient materials, including medical records and tissue specimens, and does not involve direct interaction with individuals. While the data can be encrypted, researchers and epidemiologists need to link this data back to individuals in order to generate meaningful conclusions regarding the benefits and adverse outcomes of particular treatments, as well as medical effectiveness. The question for breast cancer advocates is under what situations would it be appropriate to allow the disclosure of health information for research purposes without patient authorization.

Currently, under the Common Rule, research organizations conducting federally funded or regulated research projects must establish and operate institutional review boards (IRBs), which are responsible for reviewing research protocols and for implementing federal requirements designed to protect the rights and safety of human subjects. No human-subjects research may be initiated, and no ongoing research may continue, in the absence of IRB approval. Integral to conducting research under the Common Rule is a requirement that there is proper informed consent and documentation of that consent. There are, however, circumstances when the IRB can waive informed consent (the Common Rule). These circumstances are when the IRB finds and documents that the research: (1) involves no more than minimal risk to subject; (2) won't adversely affect the rights and welfare of subjects; (3) research can't be carried out without the waiver; and (4) whenever appropriate, subjects will be given more information after participation. Much of the research relying on medical records would meet this test. In fact, research that relies solely on medical records databases or pathology specimens may be reviewed in an expedited fashion by the IRB.

While the IRBs are not without problems and the informed consent process is far from perfect, NBCC believes this is an appropriate paradigm to build upon. IRBs have also been given the responsibility to ensure there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data and ensure protections for individuals involved in research. We believe that it would be appropriate to disclose protected health information for health research without obtaining authorization if the Secretary requires that all health research be reviewed by an IRB or an IRB-like entity ("internal privacy board"). In addition, we would like to see that all internal privacy boards meet current requirements for an IRB with respect to information protection, use, and disclosure, and are determined to be qualified to assess and protect the confidentiality of protected health information. Also, the regulations should provide that there be equal oversight and accountability for both IRBs and privacy boards.

Only under these circumstances would it be appropriate to waive authorization. NBCC acknowledges that internal privacy boards have drawbacks -but they appear to be an acceptable alternative to an IRB.

Generally, we support the intention with regard to research in the draft regulation. The regulation reflects NBCC's position that there should be uniform rules for researchers regardless of the source of funding. We also support the four proposed additional waiver criteria that IRBs and privacy boards must consider: (1) the research would be impracticable to conduct without the individually identifiable health information; (2) the research project is of sufficient importance to outweigh the intrusion into the privacy of the individual whose information would be disclosed; (3) there is an adequate plan to protect the identifiers from improper use and disclosure; and (4) there is an adequate plan to destroy the identifies at the earliest opportunity consistent with the conduct if the research, unless there is a health or research justification for retaining identifiers. These additional criteria emphasize the need for protecting privacy.

While NBCC believes that the Secretary's proposed rules attempt to create a balance between privacy and research, there are certain limitations with regard to researchers. Mainly, the draft regulation only addresses the use and disclosure of "protected health information" by covered entities. Researchers who generate their own health information fall outside the scope of the regulations if they are not based within a covered entity, and do not provide health care. We understand that this reflects the legal constraint imposed on HHS by the HIPAA. Since a great deal of research will continue to fall outside the scope of federal regulation, we believe that there is still an important role to be played by Congress to fill this gap.

2. Individually identifiable health information must be afforded greater privacy protection when it is used or disclosed for research that is unrelated to health care. (Section 164.508 (a) (3) (iv) (B))

NBCC recognizes the importance of allowing researchers to conduct vital biomedical research. The proposed regulations draw a distinction between research information that is related to the delivery of care, such as information handled in therapeutic clinical trials, and that which is not related to treatment, such as early gene sequence analysis. Research information that is unrelated to health care is: (1) received or created by a covered entity in the course of conducting research; (2) information for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care; and (3) payment is not, or has not, been requested from a health plan. The distinction has been drawn so that individually identifiable health information is afforded greater privacy protection when it is used or disclosed

for purposes that are unrelated to health care. Under the proposed rule, research information unrelated to health care generally may only be used or disclosed with authorization.

We believe that the Secretary has properly drawn this distinction. However, the definition of "research information unrelated to treatment" should be revised to ensure that once information is classified as such, it cannot be re-classified as something else at a later date. We believe that without qualifying language this information would be vulnerable to disclosure in the future, if the information were later to become of scientific validity. The regulation should be clear that once information is considered "research information unrelated to treatment" it remains that way. This is especially important given that "research information unrelated to treatment" is afforded a higher degree of protection under the proposed regulation. Individuals may rely on this higher degree of confidentiality when consenting to the collection of the information in the first instance. This confidentiality should not be betrayed in the future just because the utility of the information has changed.

The regulations should preempt state privacy laws that provide less stringent protections and should not preempt strong state privacy laws. (Section 160.203)

NBCC supports preemption if it sets a floor for the states and not a ceiling. We should not force states that have established strong privacy laws to adopt a lower standard. The proposed regulations reflect this position. The rule will preempt state laws that are in conflict with the regulatory requirements and that provide less stringent privacy protections, but will not preempt state laws that are more stringent.

Enforcement of Medical Privacy Standards must include a private right of action for individuals.

Most importantly, we believe that there should be strong criminal and civil penalties for intentionally or negligently using individually identifiable health information. While HIPPA granted the Secretary the authority to impose civil monetary penalties and criminal penalties pursuant to the proposed regulations, it did not provide for a private right of action for individuals. NBCC's position is that the key to enforceability is a meaningful private right of action -individuals must have the right to sue if their privacy rights are violated. Only strong enforcement will give people confidence that their health information is protected and ensure that those holding health information take their responsibilities seriously.

Appropriate safeguards against misuse are necessary to help build public trust. Only if women trust that their individual health information will be kept private, will they be willing to participate in research efforts. At a time when new advances in science depend heavily on participation in clinical research, we cannot let the opportunity to build public trust go by. Knowledge about how to prevent and cure breast cancer will only come if real federal standards for medical privacy are enacted.

We respectfully request that HHS reexamine and redefine its current proposal, and hope to have the opportunity to work with HHS and Congress on improving federal medical privacy standards.

Sincerely,

FRAN VISCO
President

Statement of Judith L. Lichtman, President, National Partnership for Women & Families

The National Partnership for Women & Families is a national advocacy organization dedicated to improving the lives of women and families. Improving access to high quality health care is an integral part of our mission. Privacy of medical information is an essential component of high quality care. Medical privacy is especially important to women because they are the greatest users of health care services and because of their need for sensitive services like reproductive health and mental health services. Medical privacy is also especially important to women who are victims of domestic violence because inappropriate disclosures can threaten their personal safety and that of their children.

Without confidence that private information will remain just that—private—women are reluctant to share information with their health care professionals—to

the detriment of their own health. Fear that medical information is not kept confidential also keeps women from obtaining health care services in the first place or forces them to go outside their health plan and incur significant out-of-pocket expenses.

In recognition of our leadership on women's health issues and keen interest in medical privacy, the National Partnership was asked to become a member of the steering committee of the Georgetown University Medical Center, Health Privacy Project's Consumer Coalition. As an active member of the steering committee, we helped develop the coalition's privacy principles. We applied these principles in our analysis of the proposed rule on medical privacy issued by the Department of Health and Human Services on November 3, 1999.

Strong and enforceable privacy protections are needed now more than ever thanks to the recent changes in our health care system. The rise of managed care means that more people have access to a person's medical information. The computer revolution makes immediate transfer and disclosure of such information possible, but also brings with it the possibility of strong safeguards against inappropriate use and disclosure (e.g., the need for passwords to access files).

We had hoped that Congress would meet its own self-imposed deadline of August, 21, 1999, and enact comprehensive privacy legislation. Unfortunately, Congress failed to meet that deadline.

We applaud the Department of Health and Human Services (HHS) for stepping up to the plate and promulgating this proposed rule. The promulgation of this proposed rule represents an extremely important step in restoring confidence in the privacy of health information. There are many positive features of this proposed rule that we discuss in our formal comments to HHS, as well as areas where we urge the Department to revise its approach. But even if the Department adopted all of our recommendations, Congress would still need to act. For example, the proposed rule cannot, and does not, reach all of the people or entities that use or transfer medical information. Nor does it provide meaningful enough remedies for people whose privacy rights are violated. These holes can only be fixed by Congress, and we call upon Congress to enact legislation to fill in these holes.

Some of the features of the proposed rule that we believe are especially important are the following:

- that individuals will have the right to see and copy (and supplement) their own health information;
- that individual authorization will be required for many uses and disclosures of protected health information;
- that psychotherapy notes will get the benefit of special protections;
- that only the "minimum necessary" to accomplish the intended purpose of the use or disclosure will be used or disclosed;
- that individuals will be considered "intended third party beneficiaries" of any contract between a covered entity and its business partners, thus able to enforce their own privacy rights if this contract is breached;
- that the Department has attempted to establish uniform rules for researchers, regardless of the source of the funding for the research; and
- that, in most instances, the federal rules will operate as a "floor," not a "ceiling," leaving states with the authority to provide greater protection for privacy.

There are many areas where we believe the Department can, and should, more fully protect privacy. One primary improvement would be to clarify the responsibilities of employers that sponsor covered health plans. Since most women and families get their insurance through employment, they fear that employers know more than they should about their private medical information and may use that information inappropriately to make employment decisions. Unless the Department's rule reaches employers to the fullest extent possible, America's women and families will not believe their privacy has truly been protected. In addition, a few of our other recommendations include the following:

- requiring individual authorization for treatment, payment, and health care operations purposes;
- creating a special authorization process for certain disclosures about sensitive services;
- better protecting the personal safety of victims of domestic violence, including children who are victims of abuse; and
- improving the way the proposed rule handles the rights of minors.

We look forward to working with the Administration and Congress to improve the quality of health care and to protect the privacy of medical information.

Statement of Hon. Ron Paul, a Representative in Congress from the State of Texas

Mr. Chairman, I wish to thank you for having this timely hearing on the Department of Health and Human Services' medical privacy proposal. I also appreciate the opportunity to share my reasons for opposing HHS' proposal with the Committee.

While I have several serious objections to certain parts of HHS' proposal, Mr. Chairman, my main objection to these rules is with the underlying principle of allowing a federal agency to establish one uniform medial privacy rule for all Americans. Protecting medical privacy is a noble goal, however, the federal government is not constitutionally authorized to mandate a uniform standard of privacy protections for every citizen in the nation. Rather, the question of who should have access to a person's medical records should be determined by private contracts between that person and their health care provider.

Unfortunately, government policies encouraging citizens to rely on third-party payors for even routine heath care expenses has undermined the individual's ability to control any aspect of their own health care, including questions regarding access to their medical records. All too often, third-party payors use their control over the health care dollar to gain access to even the most personal details of an individual's health care, using the justification that because they are paying for the treatments they must have access to the patient's medical records to protect against fraud or other malfeasance. Because most of the concerns about medical privacy are rooted in the loss of individual control over the health care dollar, the solution to the loss of medical privacy is to empower the individual by giving them back control of their health care dollar. The best way to do this is through means such as Medical Savings Accounts and individual tax credits for health care. When the individual has control over their health care dollar, they can control all aspects of their health care—including who should have access to their medical records.

Rather than support efforts to place the individual back in control of health care, this administration and many in Congress have pursued an agenda that would enhance the power of the federal government over health care. HHS' proposed medical privacy regulations continue in that sad tradition.

In the name of protecting privacy, HHS has reduced the individual's control over their medical records. HHS' proposal, if enacted, would deny, as a matter of federal law, individuals the ability to contract with the providers or payors to establish limitations on who should have access to their medical records. Instead, every American will be forced to accept the privacy standard decided upon by Washington-based bureaucrats and politicians.

Individual citizens would not only have to accept the privacy standards dictated to them by Washington bureaucrats, they would even be deprived the ability to hold those who violated their privacy accountable in a court of law. Instead, the regulations give the Federal Government the power to punish those who violate these federal standards. Thus, in a remarkable example of government paternalism, individuals are forced to rely on the good graces of government bureaucrats for protection of their medical privacy. These regulations also create yet another unconstitutional federal crime, at a time when voices from across the political spectrum are decrying the nationalization of law enforcement.

HHS appears to believe that the American people should accept the privacy protections designed by the "experts" in Washington. There is no other explanation for the obstacles placed in the path of those seeking to comment on this regulation. For example, HHS is refusing to accept faxed comments. Furthermore, the web site that HHS has established to accept comments is very difficult to use and does not even let the user know whether or not HHS has received his comments! Mr. Chairman, should we trust an agency that shows such a reluctance to hear the voice of the people with the power to determine medical privacy rules for all Americans?

These so-called "privacy protection" regulations not only strip individuals of any ability to determine for themselves how best to protect their medical privacy, they also create a privileged class of people with a federally-guaranteed right to see an individual's medical records without the individual's consent. For example, medical researchers may access a person's private medical records even if an individual does not want their private records used for medical research. Although individuals will be told that their identity will be protected the fact is that no system is fail-safe. I am aware of at least one incident where a man had his medical records used without his consent and the records inadvertently revealed his identity. As a result, many people in his community discovered details of his medical history that he wished to keep private!

Forcing individuals to divulge medical information without their consent also runs afoul of the Fifth Amendment's prohibition on taking private property for public use without just compensation. After all, people do have a legitimate property interest in their private information; therefore restrictions on an individuals ability to control the dissemination of their private information represents a massive regulatory taking. The takings clause is designed to prevent this type of sacrifice of individual property rights for the "greater good."

In a free society such as the one envisioned by those who drafted the Constitution, the federal government should never force a citizen to divulge personal information to advance "important social goals." Rather, it should be up to the individuals, not the government, to determine what social goals are important enough to warrant allowing others access to their personal property, including their personal information. *To the extent these regulations sacrifice individual rights in the name of a bureaucratically-determined "common good," they are incompatible with a free society and a constitutional government.*

HHS' "medical privacy" proposals also endangers the privacy of Americans by allowing law enforcement and other government officials access to a citizen's private medical record without having to obtain a search warrant. This is a blatant violation of the Fourth Amendment to the United States Constitution, which protects American citizens from warrantless searches by government officials. The requirement that law enforcement officials obtain a warrant from a judge before searching private documents is one of the fundamental protections against abuse of the government's power to seize an individual's private documents. While the fourth amendment has been interpreted to allow warrantless searches in emergency situations, it is hard to conceive of a situation where law enforcement officials would be unable to obtain a warrant before electronic medical records would be destroyed.

The proposal's requirement that law enforcement officials submit a written request to doctors, hospital and insurance companies before they can access private medical records is a poor substitute for a judicially-issued warrant. Private citizens are more likely to want to cooperate with law enforcement officials than are members of the judiciary, if for no other reason than because hospital administrators, insurance company personnel, and health care providers will lack the time and expertise to properly determine if a government officials' request is legitimate. Furthermore, private citizens are more likely to succumb to pressure to "do their civic duty" and cooperate with law enforcement—no matter how unjustified the request—than members of the judiciary.

I also object to the fact that these proposed regulations "permit" health care providers (many of whom are beholden to government funding) to give medical records to the government for inclusion in a federal health care data system. Such a system would contain all citizens' personal health care information. History shows that when the government collects this type of personal information the inevitable result is the abuse of citizens' privacy and liberty by unscrupulous government officials. The only fail-safe privacy protection is for the government not to collect and store this type of personal information.

The collection and storing of personal medical information authorized by these regulations may also revive an effort to establish a "unique health identifier" for all Americans. As you are no doubt aware, Mr. Chairman, a moratorium on funds for developing such an identifier was included in the HHS' budget for fiscal years 1998 and 1999. This was because of a massive public outcry against having one's medical records easily accessible to anyone who knows their "unique health identifier." The American people do not want their health information recorded on a database and they do not wish to be assigned a unique health identifier. Congress must head the wishes of the American people and repeal the statutory authority for HHS to establish a "unique health identifier" for all Americans.

As an OB–GYN with more than 30 years experience in private practice, I am very concerned by the threat to good medical practice posed by these regulations. The confidential physician-patient relationship is the basis of good health care; oftentimes effective treatment depends on patients' ability to place absolute trust in his or her doctor. The legal system has acknowledged the importance of maintaining physician-patient confidentiality by granting physicians a privilege not to divulge information confided to them by their patients.

Before implementing these rules or passing any legislation related to medical privacy, HHS and Congress should consider what will happen to that trust between patients and physicians when patients know that any and all information given their doctor may be placed in a government database or seen by medical researchers or handed over to government agents without a warrant?

Questions of who should or should not have access to one's medical privacy are best settled via contract between a patients and a provider. However, the govern-

ment-insurance company complex that governs today's health care industry has deprived the individual patients of control over their health care records, as well as over numerous other aspects of their health care. Rather then put the individual back in charge of his or her medical records, the Department of Health and Human Services proposed privacy regulations give the federal government the authority to decide who will have access to individual medical records. These regulations thus reduce individuals' ability to protect their own medical privacy.

These regulations violate the fundamental principles of a free society by placing the perceived "societal" need to advance medical research over the individuals right to privacy. They also violate the Fourth and Fifth Amendments by allowing law enforcement officials and government -favored special interests to seize medical records without an individual's consent or a warrant and could facilitate the creation of a federal database containing the health care data of every American citizen. These developments could undermine the doctor-patient relationship and thus worsen the health care of millions of Americans.

In conclusion, Mr. Chairman, I recommend that Congress embrace meaningful protection for medical privacy by empowering individuals to protect their medical records by repealing the statutory authorization for the Department of Health and Human Services to impose a one-size-fits all "privacy"standard on all Americans and passing legislation placing patients back in control of the health care system.

Statement of the Physician Insurers Association of America, Rockville, MD

Thank you for the opportunity to comment on the proposed regulations to implement standards governing the privacy of individually identifiable health information as directed under section 262 of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or the "Act"). The proposed rule appears to be drafted to address considerations involving health care providers and other "covered entities" that are the primary repositories of individually identifiable health information. However, the proposed rule would also impact professional liability insurers primarily due to the contractual restrictions placed on "business partners."

Interest of the Physician Insurers Association of America (PIAA)

The PIAA is a trade association of more than 55 professional liability insurance companies owned and/or operated by doctors and dentists. Collectively, these companies insure approximately 60 percent of America's practicing physicians, as well as dentists, hospitals, and other health care providers. As such, PIAA member insurance companies routinely receive reports from providers when adverse outcomes occur where no claim for recompense has yet been made. These "event or incident reports," as they are known, usually contain individually identifiable health information. Such important information is treated with the strictest confidentiality, and is rarely transmitted to anyone outside of the insurance company.

While the PIAA and its members strongly support appropriate privacy protections for individually identifiable health information, we have several significant concerns regarding the scope of the proposed rule, its liability implications and the significant costs and burdens of complying with the proposed regulations.

Application to Business Partners

The provisions contained at section 164.506(e) of the proposed rule governing the rule's application to business partners of covered entities are the source of concern for the PIAA in two significant respects.[1] First, this section of the proposed rule purports to regulate indirectly business partners that the agency has acknowledged it lacks the authority to regulate directly. Second, section 164.506(e)(2)(ii)(A)'s requirement that these contracts designate "individuals whose protected health information

[1] Section 164.504 defines "business partner" as "a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity." The proposed rule identifies "lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities" as examples of business partners for purposes of the proposed rule. Although not specifically mentioned, the PIAA believes that professional liability insurers would meet the definition of "business partner" for purposes of the rule, and assumes that professional liability insurers are so classified for purposes of these comments.

is disclosed" pursuant to the contract as explicit third party beneficiaries, thereby creates potential liability under state law.

Turning to the first concern, Congress expressly set forth those entities to be covered by the regulation in section 1172(a)(1) of the Act. Indeed, the preamble to the proposed rule acknowledges that "we do not have the authority to apply these standards directly to any entity that is not a covered entity...[w]e would attempt to fill this gap in our legislative authority in part by requiring covered entities to apply many of the provisions of the rule to the entities with whom they contract for administrative and other services."[2] Using mandated contractual arrangements to extend the reach of the regulation to parties not contemplated by Congress exceeds the authority delegated to the agency by statute. The PIAA believes that the agency should reconsider this course and allow covered entities to determine for themselves how best to fulfill their responsibilities under the Act in their relations with business partners and others. The agency should not attempt to usurp Congressional authority through the use of the contractual artifice included in the proposed rule.

For instance, section 164.506(e)(2)(i)(H) of the proposed rule would specify that, "At the termination of the contract, the business partner must return or destroy all protected health information received from the covered entity."[3] This proposed requirement fails to recognize that many professional liability contracts terminate every 12 months at which time a new contract may be offered to a provider. A decision to offer the provider a new insurance contract would certainly involve a review of past claims and adverse event experience beyond the previous 12 months. Likewise, a claim may be filed against that provider long after the contract has terminated. In this case, information about the provider's claims history or the adverse event in question may be impossible to recreate, yet would be extremely important to a prompt resolution of the claim. Under a "claims-made" policy, the notice of an event often triggers the attachment of insurance coverage for the claim should it be reported in the future. For this reason and others, covered entities and their business partners should define the terms and conditions of their contracts instead of having them dictated in regulations.

Additionally, the PIAA is concerned that the proposed rule contains a requirement that covered entities and their business partners designate individuals whose protected health information is disclosed as express third party beneficiaries by contract. While the agency proffers no reason for the inclusion of this requirement in its discussion of the proposed rule, several experts in the area of health law have suggested that this provision creates the potential for private rights of action utilizing a third party beneficiary theory under state law.

As the agency has itself acknowledged, HIPAA (passed by the 104th Congress) makes no provision for a private right of action by individuals for violations of the statute.[4] This should be regarded as an affirmation that civil and criminal penalties are the sole remedy for the unauthorized release of a patient's confidential health information. Moreover, the question of whether to include such a private right of action has been bitterly contested in deliberations by the 106th Congress over legislation that would provide broader privacy protections of individually identifiable health information. Given the absence of any congressional establishment of a federal cause of action for the violation of rights created under the statute, the Agency should not attempt to create a potential private right of action. The PIAA is gravely concerned that the agency would see fit to require the inclusion of provisions creating liability under state law in these contracts, particularly without any discussion of the potential liability ramifications of the third party beneficiary designation.

In addition to these specific concerns, we believe that the application of this rule to business partners will result in expenditures of significant resources for marginal additional improvements in privacy protection. This would occur at a time when health care expenditures continue to rise and there is a serious interest in decreasing the incidence of medical errors and improving patient care. Devoting resources to the establishment of appropriate privacy protections for individually identifiable health information must not be considered in isolation, but rather as one element in improving the current health care system.

We are similarly concerned with the prospect of an increasingly confusing and possibly conflicting array of responsibilities for liability insurers in the area of privacy. Has the Agency considered in detail the interaction of the "business partner" rule with privacy obligations that may arise under other proposed regulations and

---

[2] See 64 *Fed. Reg.* p.59924, (Nov. 3, 1999)

[3] See 64 *Fed. Reg.* p.59924, (Nov. 3, 1999)

[4] See 64 *Fed. Reg.* p.59918, p.59923 (Nov. 3, 1999) ["In HIPAA, Congress did not provide such enforcement authority. There is no private right of action for individuals to enforce their rights. . ."]

recently enacted legislation such as the Financial Services Modernization Act. We believe that minimizing cost and confusion, as well as eliminating any potentially conflicting obligations is central to effectively protecting patient privacy.

The PIAA urges the agency not to utilize mandated contractual arrangements to improperly enlarge on the narrower authority granted by Congress, and in particular to withdraw the requirement that the third party beneficiary designation be included in such contracts.

Customary Business Relationships in the Health Care Industry

During our review of the proposed rule, PIAA members raised concern regarding the potential impact of the proposed rule on liability insurers' access to individual health information related to the activities of their insureds. The preamble to the rule indicates that the Agency intends "to allow customary business relationships in the health care industry to continue." As part of current normal business practice, professional liability insurers typically receive individually identifiable health information related to adverse incidents that may give rise to claims against an insured. Indeed, reporting requirements are typically stipulated as part of the claims made policy in an insurance contract. Sharing of such information also allows the liability insurer to conduct underwriting reviews to determine insurability. Finally, such an open business relationship promotes consideration of how health care systems can be improved to prevent recurrent adverse events. Under the proposed rule, it is unclear under what conditions this transfer of information could take place without individual authorization.

Under section 164.506(a) as proposed, a covered entity would be permitted to use or disclose protected health information without individual authorization for treatment, payment or health care operations. "Health care operations" as defined under proposed section 164.504 includes:

"(3) Insurance rating and other insurance activities relating to the renewal of a contract for insurance including underwriting, experience rating and reinsurance, but only when the individuals are already enrolled in the health plan conducting such activities and the use or disclosures of the protected health information relates to an existing contract of insurance (including the renewal of such contract);

(5) Compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding."

The PIAA is concerned that the proposed definition of "health care operations" fails to include the sharing of information with professional liability insurers that is both current business practice and necessary for risk management, error prevention, improving patient care, underwriting and other insurance purposes. The discussion of insurance under the proposed definition (above) appears to be limited to insurance provided by health plans and does not expressly contemplate other types of insurance, such as professional liability insurance.

The aspect of the definition including information compiled "in anticipation of litigation," similarly provides little comfort as it fails to embrace the full array of situations in which individual health information must be exchanged between an insured and a professional liability insurer. This exchange of information often occurs long before a civil or criminal action is indicated, and indeed is necessary to allow the insurer to investigate the incident and determine whether compensation should be paid before any demand letter is received or civil action initiated. This exchange of information is additionally necessary even when no claim is made to aid in underwriting and risk management/evaluation activities.

Moreover, the "in anticipation of or for use in a civil or criminal proceeding" standard is quite similar to, and equally as vague as, the "anticipation of litigation" standard for the work product rule under Federal Rule of Civil Procedure 26(b)(3) which has spawned reams of case law attempting to define under what circumstances this standard has been met.

The ramifications of failing to clarify the definition of "health care operations" to include information shared with professional liability insurers are serious as it would appear that professional liability insurers would then be relegated to the exception for protected health information obtained for judicial and administrative proceedings. As proposed, the rule would impose the burdensome requirement that any transfer of protected health information could only occur pursuant to court order or by request from legal counsel in litigation. This result would be counterproductive for all concerned, including patients, as it would essentially require litigation in order for the claim to be evaluated. The current practice of sharing information with the professional liability insurer as soon as an adverse incident occurs facilitates compensation without litigation in many instances and results in lower costs per claim.

In light of the foregoing, the PIAA would respectfully request that the agency modify the definition of "health care operations" to make clear that protected health information could be shared with a provider or other covered entity's professional liability insurer without prior authorization.

Finally, we would like to commend the Agency for a well-detailed and thoughtful approach to creating protections in a new and difficult area. We hope that our comments will be addressed in any further actions the Agency takes regarding this matter.

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

Mr. Chairman, thank you for calling this important hearing to review the Administration's proposal to protect the confidentiality of medical records.

Given the sensitive nature of personal health records, I am very aware of the importance of crafting appropriate rules and regulations, as well as the complexities that surround this task.

I applaud the efforts of the Secretary to tackle this important issue with a comprehensive framework to protect patient information without inhibiting the use of data to continue research into life-saving and life-enhancing treatments, drugs, technologies and procedures. Ensuring regulations are balanced and do not stifle research, while protecting privacy, is one of my top priorities.

Given the vast expanse of the regulations and the number of health care providers impacted by them, this hearing is important to closely examine the rules and determine if changes are necessary or more work needs to be done legislatively.

I welcome this opportunity to learn more from today's witnesses on this significant health care issue, and I thank you again, Mr. Chairman, for calling this important hearing.

Testimony of the Hon. Louise McIntosh Slaughter, a Representative in Congress from the State of New York

I thank you, Chairman Thomas and Representative Stark, for this opportunity to testify on one of the most critical issues in Congress: medical records privacy. I cannot tell you how pleased I am that Congress is finally taking up this matter in earnest.

It is truly gratifying for me to see a national consensus emerging on the need to protect the privacy of medical records. Privacy is one of the bedrock principles of our Constitution and a pillar of our democracy. Our Founders considered privacy so important that they included it in the Constitution in several different forms. The First Amendment protects our right to express our private thoughts, and our right to associate in private or public with whomever we choose. It protects the privacy of one's home, possessions and person against unreasonable search and seizure. It therefore seems natural that the privacy of medical records—which contain the most personal of information about an individual—should also be protected.

Unfortunately, Americans' medical records are anything but private. While many people believe their medical records are closed to everyone except their health care provider and insurer, the truth is very different. On February 4, 1997, a New York Times article recounted how one doctor started investigating how many people had access to his patients' records after being confronted with one patient's fear of disclosure. He said, and I quote, "I stopped counting at 75." This incident happened a decade ago. The situation is even more extreme today.

Doctors, nurses, therapists, and secretaries are only a few of the people who have access to an individual's medical charts. Today our medical records may also be viewed by consultants, billing clerks, insurance "coders," and many others. An employer may have free access to workers' records, especially if the company is self-insured. Medicare sees the records of elderly and disabled patients, while Medicaid workers may view medical charts for the poor. The potential for genetic discrimination and other misuse of this information is staggering.

The computerization of medical records has exacerbated this situation. Many insurers pool medical information in the Medical Information Bureau, which may distribute it to any number of sources. Marketers buy sophisticated lists of health and demographic information to help them target their products. Lawyers look at

records in the context of rape, domestic violence, and medical injury cases. Equifax and other credit reporting services can also get access. The list goes on and on.

The computerization of medical records has added a new urgency to the need for regulations to protect consumers. In the past, the practical limitations of paper records made access more difficult. Computerization of records means that large numbers of medical records can be screened, collated, and distributed in the blink of an eye. Information can be made available to almost unlimited numbers of people via the Internet. The market for medical records information is booming, and there is reputed to be a vigorous black market for it as well.

With the advent of computerized records, the potential for malicious misuse of this information is truly appalling. In a widely publicized case, a Florida public health official was fired after allegedly mailing computer disks with the names of thousands of Florida patients with HIV and AIDS anonymously to Tampa-area newspapers. This individual also reputedly took a list of the patients into a local bar and offered to help friends screen potential dates. In 1996, the Baltimore Sun reported that in Maryland there had been examples of state employees accepting bribes from HMOs for information on Medicaid recipients. One Delaware banker obtained a list of cancer patients, cross-referenced it with loan customers at his bank and called in those loans.

There is a clear and pressing need for federal legislation to protect the privacy of our medical records. In a 1997 review of state medical privacy and confidentiality laws prepared for the Centers for Disease Control and Prevention, the Electronic Privacy and Information Center (EPIC) called federal privacy laws "fragmented and uncertain." As long ago as 1994, the Institute of Medicine endorsed passage of comprehensive federal legislation to replace the patchwork of laws that cover medical records. According to the EPIC report,

Thirty-seven states impose on physicians the duty to maintain the confidentiality of medical records. Twenty-six extend this duty to other health care providers. Thirty-three states and territories require health care institutions to maintain the confidentiality of medical records they hold. The survey found that only four states have specific legislation imposing this duty on insurers, despite the vast amount of information held by insurance companies. Nine states impose a similar duty on employers or other non-health care institutions.

Only twenty-two states have legislative provisions that protect computerized or electronically transferred data. Forty-two states protect information received during the course of a physician-patient relationship from disclosure in court proceedings, with certain exceptions. Twenty-eight states provide statutory penalties for unauthorized disclosure of health care information. Twelve impose criminal penalties, nineteen create civil penalties and three allow for both civil and criminal penalties. Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization, EPIC, February 1997.

The report concludes by endorsing passage of federal privacy legislation, stating, "Uniform standards nationwide will result in more effective protection of health information privacy."

The situation has changed little since that 1997 report. State laws are fragmented and inconsistent. People living on opposite sides of a state line have widely divergent privacy protections and recourse against violations.

In attempting to fulfill the Health Insurance Portability and Accountability Act of 1996's (HIPAA) requirement that Congress pass medical records privacy legislation, we all learned a difficult lesson about the many competing interests on this issue. The medical records privacy debate draws in virtually every fact of the health care industry -doctors, nurses, hospitals, nursing homes, insurance companies, blood banks, tissue banks, laboratories, information processing firms, pharmaceutical companies, private and university-based researchers, disease advocacy groups, medical schools, and more. Many of these entities have very different ideas about the appropriate level of privacy that should be afforded to medical records. And first and foremost, we must consider the concerns of individual Americans.

Today's hearing seeks to examine the recent regulations promulgated by the Department of Health and Human Services on the privacy of computerized medical records. In the broadest sense, these regulations are a major step forward. They represent the first concerted federal effort to ensure that Americans' medical information is not treated lightly. I commend Secretary Shalala and the HHS officials responsible for producing these regulations for their extremely hard work. I would like to highlight three concerns raised on the regulations:

Research Must Not Be Inhibited. As a former microbiologist, I am keenly aware of the challenges faced by researchers in obtaining, analyzing, and interpreting medical information. Legitimate scientific studies should not be hampered by overly burdensome requirements or regulations. It is my firm belief that the major-

ity of research can and should be conducted with medical information that is not individually identifiable. Further, I am deeply concerned that some industries may attempt to obtain medical records for marketing purposes under the guise of "research." The regulations must ensure that science can move forward without compromising the privacy of individuals.

Authorization and Consent Forms Must Be Meaningful. Today, most insurance forms contain a blanket consent paragraph that the individual must sign or risk being denied coverage for treatment. I am pleased that the regulations are designed to end these meaningless, coercive authorizations and replace them with a more targeted, informative system. The authorization form content requirements in the HHS regulations are a major step in the right direction. We must, however, ensure that consumers are not presented with endless paperwork, printed in small type and written in bureaucratic jargon. Such a case would only result again in consumers signing forms without reading them or reviewing their private rights in a meaningful fashion.

Effectiveness of the Regulations Should Be Studied. I would strongly encourage HHS to include explicitly with the regulations one or more studies of their effectiveness. Which consent forms are the most useful for consumers? Are individuals indeed reading authorizations and considering their privacy rights? Are entities which hold medical records complying with the spirit as well as the letter of the law? Where are the remaining loopholes that may not have been anticipated? Is research being impacted adversely? Are certain requirements too burdensome? These regulations are complex; we cannot allow them to be issued without thoughtful oversight of their impact.

Finally, I would like to raise a related issue that must not be ignored. While medical records privacy is critically important, it is only one side of the coin. The other side of the coin is nondiscrimination. Individuals' private medical information, and in particular their genetic information, should not be used to harm them. Without nondiscrimination laws, privacy is an empty protection. Without privacy protection, nondiscrimination laws are unenforceable.

I am proud to be a leader in Congress in the effort to ban genetic discrimination. In 1995, I introduced legislation to ban genetic discrimination when few Members were even aware of the Human Genome Project. Today genetic research and discoveries are the subject of seemingly daily press reports. A "rough draft" of the entire human genome will be completed this spring. Over the past five years, I have worked consistently to keep these issue before Members of Congress, educating them and their staffs about the many ethical, legal and social implications of genetic research.

H.R. 306, the Genetic Information Nondiscrimination in Health Insurance Act, would prohibit insurers from denying, canceling, refusing to renew, or changing the rates, terms, or conditions of coverage based on genetic information. This bill has the overwhelming support of 212 bipartisan cosponsors and over 100 health-related organizations. I am proud to count as cosponsors all of the Health Subcommittee Democrats, as well as Rep. Nancy Johnson.

More recently, I have introduced H.R. 2457, the Genetic Nondiscrimination in Health Insurance and Employment Act. As its title suggests, this bill would ban discrimination in both health insurance and employment. Just last week, President Clinton endorsed this legislation in a major Administration event and signed an executive order banning genetic discrimination in federal employment.

Unfortunately, the new HHS medical records privacy regulations do not ban genetic discrimination. Doing so would have exceeded the scope of the HIPAA mandate. It is therefore up to Congress to act on this critical issue.

We owe it to the American people to ban genetic discrimination. Throughout the course of my work on this issue, I have received heartbreaking letters from people who want to take a genetic test, but have decided not to do so because they are afraid the results might be obtained by their health insurer or employer. Whenever I speak to groups about genetics, I am inevitably approached by people afterwards who describe their own family history of illness and their fears that this information will be used against them. It is absolutely reproachable that Congress is allowing this situation to persist for millions of Americans simply because the leadership will not act upon this issue.

Medical records privacy is long overdue. Again, I commend Secretary Shalala and her staff for producing excellent draft regulations. With some changes, these regulations will provide a solid basis for protecting the privacy of medical information in this nation. The next step must be to protect Americans against genetic discrimination. Unless we ensure that this information cannot be used to undermine individuals' best interests, the public will rightly stop supporting genetic research. The enormous promise of genetic technology will then go unfulfilled.

I appreciate having this opportunity to offer my comments on medical records privacy issues, and I look forward to working with the members of the subcommittee to ban genetic discrimination.

Statement of VHA Inc.

On behalf of the membership of VHA, we submit these comments on the Administration's proposed regulations regarding privacy of individually identifiable health information. VHA supports the idea that an individual's medical information should remain confidential. However, this confidentiality should not operate as a barrier to quality and efficient care. With this goal in mind, VHA offers the following comments on the proposed regulations that will have an enormous impact on all of America's hospitals.

VHA is a nationwide network of community-owned health care systems and physicians. Through shared knowledge and commitment, we build strength to improve community health and achieve market success. VHA has more than 1,800 members, representing many of America's leading community-owed health care providers, in forty-eight states and the District of Columbia. That number represents twenty-four percent of the nation's community-owned hospitals.

Patients and consumers must be assured that any use of their medical information will be appropriate and maintained as strictly confidential in the course of providing care, performing essential quality assurance activities, conducting bona fide research, complying with legal requirements, and performing specific public health activities.

VHA believes that any regulation should avoid imposing undue administrative burdens and costs on health care providers and others, or unnecessarily impeding the exchange of information used in patient care, quality, and payment. Neither should any regulation adversely impact clinical research or prudent access to research databases essential for the advancement of patient care.

It is important for health care organizations operating in multiple states to have a consistent guide for maintaining the confidentiality of patient medical information. Therefore, any federal regulation should preempt existing state laws to ensure a unified law for multi-state operating health care organizations.

Patient-identifiable health information is currently used in a variety of activities to improve health care quality. These activities include health promotion and disease prevention, disease management, outcomes research, and utilization management. Computers, electronic communication and the rapidly increasing knowledge about human genetics are vastly improving quality of care. However, the widespread use of electronic technology to store, transmit, and use health record information has raised questions about the safety and security of confidential health information. It is important that patients and consumers be assured that any use of their personal medical information is appropriately maintained as confidential.

VHA aids its members in the development of sound operational efficiencies that result in both clinical and economic benefits. The federal government has long recognized the need for such efficiencies and has exhibited its commitment to encouraging them through the implementation of various prospective payment systems in the Medicare program. VHA's activities are consistent with the federal priority to require operational efficiencies at all levels in the health care industry.

To achieve its goals, VHA believes that HHS should clarify the definition of "health care operations" and include a definition of "marketing."

First, the definition of "health care operations" needs to be expanded. Under the proposed regulations, covered entities, such as VHA members, would not need to seek authorizations for uses or disclosures of protected health information ("PHI") that relate to "health care operations." As currently written, the definition of "health care operations" includes specific activities "for the purpose of carrying out the management functions of [covered entities] necessary for the support of treatment or payment." VHA applauds HHS for its recognition that uses of PHI for purposes that are "compatible with and directly related to" treatment and payment should be exempt from a general authorization requirement. While the definition of "health care operations" acknowledges this fact, some activities have been overlooked, creating ambiguities that could inhibit the nation's hospitals' ability to provide high-quality patient care and hospital efficiency.

VHA is concerned about the status of activities related to sound clinical and operational efficiencies under these regulations. One critical aspect of patient care is the ability of hospital clinicians to work together to ensure that each physician has met the hospital's goal of clinical and operational efficiency. One aspect of this team ap-

proach involves the review of the provisions of medical drugs and devices by providers. These reviews require that other members of the hospital staff have access to medical records, which include PHI. The staff members must work together with physicians to review relevant medical records to determine the most efficacious and economic drug or device for patients.

The definition of "health care operations" needs to be clarified to ensure that these types of reviews come within the tier of activities for which patient authorizations are not required.

While these reviews most likely fall within "health care operations" as one aspect of "evaluating practitioner and provider performance" or as part of internal quality oversight, the fit is not absolutely clear from the text of the proposed regulations. As the preamble notes, the intent of the regulations is "to make the exchange of [PHI] relatively easy for health care purposes." These reviews are an important health care purpose.

While VHA does not believe HHS intended to exclude these types of reviews from the definition of "health care operations," we seek clarification as to their status. Therefore, we suggest that HHS augment the definition of "health care operations" by including in the text of the regulation itself *"engaging in activities related to achieving clinical and operational efficiencies"* in subparagraph two of the definition. This clarification should be extended to the preamble as well.

The financial gain notice requirement should be narrowed. Under the proposed regulations, a covered entity must include a statement regarding the financial gain associated with a use or disclosure of PHI when the covered entity requests an authorization for the use or disclosure that will result in financial gain to the entity. In the preamble, HHS clearly describes its concerns about financial gains resulting from marketing activities.

VHA understands the concerns regarding the use of PHI for inappropriate marketing activities, but the proposed language of the regulation is too broad and restricts other necessary activities that may also result in financial gain to a covered entity. For example, when a hospital reviews a physician's prescription of drugs or use of devices for his/her patients to achieve sound clinical and operational efficiencies, the hospital, as well as the patient, the community, the federal government in its role as a payer for health care, and indeed the entire health care system receive economic gain. This goal of providing high quality clinical care that is also operationally sound is the same as that embraced by the Congress and the Administration through its creation of the prospective payment systems.

VHA does not believe HHS intended to create such an impediment to the use of sound operational efficiencies. Thus, VHA suggests that the financial gain statement requirement at 45 C.F.R. § 164.508(d)(iv) be narrowed to read: "(iv) Where use or disclosure of the requested information will result in financial gain to the entity *that is unrelated to the care of the individual or the sound clinical or operational efficiencies of the covered entity*, a statement that such gain will result." The preamble should also be modified to reflect this modification.

The "minimum necessary" standard must be tightened so as not to divert necessary resources from patients and to address, in a practical manner, the uses and disclosures of PHI in day-to-day patient care.VHA is concerned that, as currently described, the "minimum necessary" standard will inhibit the delivery of high quality, cost-effective health care. While it is clear that some uses or disclosures of PHI may not require all of the PHI located in a medical record, other uses will require this complete set of information. Because a vast number of medical records remain on paper, abstracting can be an enormous impediment to accomplishing the minimum necessary goal. Although well-intentioned, this standard will divert even more scarce resources from patient care to administrative functions.

Secondly, it is unreasonable to expect that an appointed person or group will always be able to discern the "correct" amount of information necessary for a particular purpose, especially as related to treatment and certain aspects of health care operations. For example, what might not seem important to the appointed person may become vitally important at a later date in the patient's treatment. If the information is missing, the patient's medical needs would not be met. The provider might not even realize until too late that the record he/she had received had been redacted.

VHA members involved in reviewing the provision of drugs and devices by providers could also be severely hampered. On the surface the individual determining the "minimum necessary" amount might believe that only the diagnosis and medicine prescribed is required reviewing a provider's prescription practices. For the review to meet its goals of improving clinical and operational efficiencies, however, it is often necessary to know the patients' entire histories so that reviewers can determine why a physician might have selected certain drugs or devices. Redacting

records, even with the best of intentions, may make quality reviews inefficient or completely impossible.

Thus, VHA suggests that the standard be tightened. First, it should be clear that in the case of treatment and health care operations, the minimum necessary standard should be modified. In the case of uses or disclosures for treatment, the minimum necessary standard should apply only to the number of individuals who obtain the PHI, not the amount of information because the vast majority of cases will need a full record. To do otherwise threatens patient care. For health care operations, the text already creates an exception for "audits and related purposes." This exception should be clarified so that important health management reviews of provider practices are also not subject to the standard in terms of amounts of data, but only in terms of the number of people with access to the information.

Second, the explanation of the standards describing the factors that the Secretary expects to be used in making the minimum necessary determinations should be made part of the text of the regulation. Otherwise, the standard is too vague to be workable and creates the risk that the courts who will ultimately determine the meaning of "reasonable," will rely on a different analysis.

Whistleblowers should be held to a "reasonableness" standard or not be exempt from the "minimum necessary" requirement entirely. As HHS recognizes, the role of whistleblowers has been etched into efforts to curb fraudulent behavior. VHA understands the need to allow these individuals to report abuses to health oversight agencies, law enforcement officials, or attorneys. The broad protection afforded whistleblowers in these regulations, however, erodes the protection of an individual's confidentiality, which constitutes the heart of the regulations.

VHA is troubled by this provision generally. At a minimum, we suggest that addressing three basic problems with the provision would aid in ameliorating these concerns. First, the provision currently permits an individual to disclose PHI on a "belief." This standard is too broad and unenforceable. Other areas of law traditionally focus on a "reasonableness" standard, which is stronger than that of a "belief." Under a reasonableness standard, a whistleblower would not be liable for the disclosure if a reasonable person would have evaluated the particular act as a violation of the laws. Thus, he/she is held to a societal standard that can be objectively evaluated and provides some level of protection for those whose information is disclosed. A "belief" standard, however, is subjective, making it almost impossible to find that the whistleblower erred. As noted in the preamble, a balance must be achieved so that whistleblowers are not completely discouraged from playing their vital role. This provision is not balanced, but rather lopsided and provides no check on disclosures of this type. Thus, HHS should adopt the widely accepted reasonableness standard of tort law, as the standard which provides protection for both individuals and whistleblowers, by which to judge these disclosures.

Secondly, the provision provides whistleblowers with carte blanche to disclose any amount of PHI they desire. This allowance rips away the very protection at the center of the regulations. Thus, while covered entities work diligently to protect each individual's confidentiality, their employees, without any limitations, can breach that confidentiality in the name of a "believed" abuse. VHA suggests that this provision be limited by requiring whistleblowers to apply the "minimum necessary" standard applicable to covered entities and their business partners. Whistleblowers will not be deterred because the reasonableness standard will protect them. If their calculation of the amount of PHI they disclosed was reasonable, they will not be subject to sanctions. If not, however, the employee can be reprimanded. This approach strikes the right balance that permits good faith attempts to report abuses and creates an incentive not to disclose PHI maliciously or without reason.

Third, as drafted the provision allows whistleblowers to disclose PHI to any attorney for the purpose of determining whether a violation of law has occurred. Permitting disclosures to any is extremely problematic. In addition to vastly increasing the number of individuals to whom PHI can be disclosed, it establishes no restrictions on how these attorneys can further use or disclose the PHI in the future because they are neither covered entities nor business partners and, therefore, not subject to the regulations. Thus, the protection of patient confidentiality, which is the point of this entire regulatory scheme, is severely hampered by this aspect of the whistleblower provision. VHA suggests that HHS clarify this provision to limit the entities to whom PHI can be disclosed for purposes of whistleblower activities to law enforcement officials and oversight agencies or individuals designated by the covered entity to deal with such concerns.

Taken together, these broad, subjective aspects of the whistleblower provision work to destroy the right to confidentiality HHS has attempted to craft. Thus, if maintained, this provision should be significantly revised.

Conclusion

VHA appreciates the opportunity to present its views on this important issue. We agree that "a clear and consistent set of privacy standards" are needed "to improve the effectiveness and the efficiency of the health care system." Because of the vast nature of the proposed regulations, the final regulations must present both the health care community and the individual whose PHI is being used and disclosed with a clear picture of what is required. However, these requirements should not sacrifice America's high standard of health care. Thus, VHA offers these comments as an important step in the national conversation about this issue.