ASSESSING HIPAA: HOW FEDERAL MEDICAL RECORD PRIVACY REGULATIONS CAN BE IMPROVED

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MARCH 22, 2001

Serial No. 107–15

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

71–494PS WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

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

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON HEALTH

MICHAEL BILIRAKIS, Florida, *Chairman*

JOE BARTON, Texas
FRED UPTON, Michigan
JAMES C. GREENWOOD, Pennsylvania
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
Vice Chairman
BARBARA CUBIN, Wyoming
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
JOSEPH R. PITTS, Pennsylvania
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

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

CONTENTS

ASSESSING HIPAA: HOW FEDERAL MEDICAL RECORD PRIVACY REGULATIONS CAN BE IMPROVED

THURSDAY, MARCH 22, 2001

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

The subcommittee met, pursuant to notice, at 10:05 a.m. In Room 2123, Rayburn House Office Building, Hon. Michael Bilirakis (chairman) presiding.

Members present: Representatives Bilirakis, Upton, Greenwood, Whitfield, Ganske, Norwood, Shadegg, Bryant, Buyer, Pitts, Tauzin (ex officio), Brown, Waxman, Barrett, Capps, Stupak, Engel, Wynn, Green, and Dingell (ex officio).

Also present: Representative Markey.

Staff present: Marc Wheat, majority counsel; Brent Delmonte, majority counsel; Kristi Gillis, legislative clerk; and John Ford, minority counsel.

Mr. BILIRAKIS. Can we have order please? Good morning. Today the subcommittee tackles a very complex issue, the medical records privacy rule issued last year by the outgoing administration.

This is an issue of great importance to both health care consumers and the regulated community, and we will hear the views of expert witnesses about whether the rule adequately balances the interests involved.

Americans should feel secure in knowing that their medical records are kept confidential in virtually every instance, unless disclosure of their record is authorized by the patients themselves. The best way to ensure open and honest communication between providers and patients is to guarantee that the information shared during such exchanges is kept out of the public domain.

That being said, I have concerns that the regulation issued late last year which is presently undergoing a comment period may not strike the balance appropriately. For example, some local pharmacists from our districts have said that the rule may prevent from them filling prescriptions unless they have received a signed authorization from the patient. While that requirement may sound reasonable, we must think of the elderly shut-in who needs her son or daughter to pick up her prescriptions. Under the rule, she could not get her prescriptions filled without going to the pharmacy to fill out the form and pick up the prescription in person. This may not

be difficult for most people, but it could be a major problem for a frail elderly individual.

Likewise, concerns have been raised about the burdens this may place on small rural hospitals. I am told that the rule requires them to keep written consent for 6 years. This raises several questions: Is it necessary to keep these records? Does this record-keeping requirement help or hurt patients and providers? We should be concerned if money that would otherwise be spent on patient care would be diverted to other efforts to comply with this regulation. Whether that result is likely or possible is a question we must explore today.

I would also like to explore why statutory authorization language was dropped from the proposed rule. When the Clinton administration first proposed its regulations, there was no requirement to obtain the specific consent of the patient before disclosing information for treatment and payment. In fact, the proposed rule indicated that such a requirement could impair care. Subsequently, however, this provision was replaced by a requirement to obtain specific consent. Certainly there are instances when specific consent should be required before medical information is shared with others. However, it may not be necessary in other situations, such as when calling patients, when scheduling appointments, or answering questions about medication interactions when patients call providers.

Finally, I want to address one concern up front. We will not hear today from an administration witness. When an initial inquiry was made by us, the Department of Health and Human Services indicated that it could not provide a witness to testify on the regulation until the comment period ended. We have since learned that the Department does not face any legal obstacle but, rather, that the regulation issued by the previous administration is currently under review and policy analysis by the new administration.

In light of the change in leadership at HHS and the complexity of these issues, I understand the Department's position. However, I also appreciate very much the concerns raised by a number of our colleagues. I know we will hear those concerns in opening statements this morning from members who would like to hear from the current administration on these important issues; and we all want to hear from the current administration regarding these issues.

We have asked them to provide their views on this issue at a future hearing, and we are making every effort to have that done before the April break.

In closing, I want to thank all of the witnesses who have appeared today to help educate us on this very important subject. Your input is vital to this committee's ability to ensure the Federal policies and medical records privacy truly serve the best interest of the American people.

The Chair yields to Mr. Brown for an opening statement.

Mr. BROWN. I thank you Mr. Chairman. Not to disappoint, I would like to point out that a lot of us are concerned that there is not a witness from the Department of Health and Human Services. We do welcome your willingness, in fact, to include a witness from HHS to tell their side of the story and to get the input we need from the key government agency that is working on this

issue. I am confident that this lapse in cooperation with the minority is an aberration. Our relationship has been very good and will continue to be, and we will continue to work well together.

I look forward to hearing from the impressive list of witnesses, especially John Clough of Cleveland Clinic, who are in attendance this morning. Medical records privacy, to be sure, is not a partisan issue. I am confident that every member of this subcommittee favors strong privacy rules even if we disagree on some of the specifics. And discussing the current regulation need not, and I think will not, be a partisan exercise.

Ironically, one of the major concerns I have heard about the privacy regulations is that they are too open to multiple interpretation and the world there too vague. That is another way of saying that the regulations are not prescriptive enough, that they are too flexible. You rarely hear that concern raised about government regulation generally. Still, I think it is a valid concern based on my conversations with providers and with insurers.

There are provisions that need further clarification. That can be accomplished without delaying implementation of the regulation. There may be other provisions that need to be rewritten. That, too, can be accomplished without undue delay in implementation of these privacy regulations. If at all possible, we should try to resolve any of these concerns with this legislation without undue delay in implementation.

We have need of medical privacy protections. We are almost there. And on behalf of every person who uses the health care system in this country, we should do everything in our power in this committee to complete the job.

That said, we need to listen with an open mind to the concerns raised today by providers, by insurers, and other stakeholders. In addition to concerns, I hope our witnesses will provide specific suggestions on how to address these concerns, and the more explicit the better. Again, our fundamental objective should be to publish a set of objectives that are meaningful and realistic and to do so as soon as possible. If that means modifying the current regulations, there are mechanisms to do that. We should explore those mechanisms before exposing consumers to serious breaches of their personal privacy.

I thank you, Mr. Chairman.

Mr. BILIRAKIS. I thank the gentleman. The Chair recognizes the gentleman from Indiana, Mr. Buyer, for an opening statement.

Mr. BUYER. I yield back my time.

Mr. BILIRAKIS. The Chair appreciates that. Mr. Waxman.

Mr. WAXMAN. Last year, the Clinton administration issued a medical privacy rule that provides essential protection for American families. The rule is long overdue and it is a welcome step toward establishing privacy rules that ensure the effective operation of our health care system. We should be moving forward to put this rule into effect and build on the solid foundation of privacy protections it establishes.

Unfortunately, we are now going in the wrong direction. This situation is accurately described in the title of Tuesday's USA Today editorial: Bogus Scare Tactics Delay Medical Privacy Reforms. I

would like to ask unanimous consent that this be inserted in the record.

Mr. BILIRAKIS. Without objection.

[The editorial follows:]

[Tuesday, March 20, 2001—USA Today]

BOGUS SCARE TACTICS DELAY MEDICAL-PRIVACY REFORMS

A couple of years ago, North Carolina resident Terri Seargent got a genetic test showing that she is susceptible to a respiratory disease. When her employer learned of the results, she got a pink slip.

Last year, a Maryland school board member's medical records were sent to school officials as part of an attack campaign. And more recently, a hacker downloaded medical records from patients at the University of Washington Medical Center.

All of this and much more came in the wake of Congress' decision back in 1996 to make protecting medical privacy a priority. Medical records once safely housed in doctors' offices were, lawmakers recognized, too easily collected, sold and disclosed in the Internet age. Since then, however, intense lobbying by groups that benefit from the status quo has delayed reforms, leaving sensitive medical records exposed to marketers, employers and others who want a peek.

Now those delays are being compounded by the Bush administration's decision to take a fresh look at new federal privacy rules—just weeks before they were to take effect.

The history: The 1996 law gave Congress three years to develop privacy protections. When Congress missed the deadline, the law ordered federal regulators to write rules.

Slated to take effect April 14, these regulations combat some of the worst privacy abuses. For instance, HMOs and doctors would have to tell patients who is looking at their records. They'd have to get written consent before sharing records with anyone not involved in the treatment or payment for care. And patients could see their records and fix mistakes.

Critics—mainly health insurers, pharmacists and marketers—argue that the regulations are needlessly heavy-handed and costly. They are circulating several horror stories to make their case. But most of these claims wither under scrutiny. Among them:

- that hospitals might have to build soundproof walls between patients in recovery rooms to avoid "inadvertent disclosure" of health information. Yet the rule requires only that reasonable privacy safeguards be used, such as keeping voices down.
- that husbands wouldn't be able to pick up a prescription for their sick wives because of the restrictions on access to records. But the rules specifically allow family members to pick up prescriptions.
- that quality care would suffer because of restrictions on what doctors can tell each other. However, the restrictions are lifted when data are needed for patient treatment.

More importantly, ensuring a modicum of privacy will go a long way toward improving the quality of health care. Roughly one in six patients try to protect privacy by, among other things, dodging doctors or lying to them, according to a 1999 Princeton Survey Research Associates poll. Forty percent won't give doctors online access to their medical records, a California HealthCare Foundation survey found.

Critics say the rules just need a fresh scrubbing. Indeed, the regulations could be improved. That's often the case with a new, complex set of rules. And that's why Congress specifically authorized regulators to fine-tune the privacy regulations as needed "to permit compliance."

Given their long opposition to any meaningful privacy protection, critics are more likely looking for ways to weaken the regulations. They want, for instance, a federal rule that overturns stronger state privacy mandates. The Bush administration has given them until the end of this month to voice complaints, and has indicated it might delay the regulations to accommodate them.

Five years after Congress promised better privacy protections for medical records, it's patients who need to be accommodated—not those lobbying for further delays. Today's debate: Medical records Critics work overtime to undermine pending regulations.

Mr. WAXMAN. Well-funded interest groups are engaged in concerted efforts to unravel or put off altogether the privacy protections in the rule. The administration should be focused on working

with affected parties to answer questions and issue any guidance necessary to ensure effective implementation of the rule. Instead, Secretary Thompson reopened the rule for comment, raising the possibility that implementation of the rule would be delayed beyond the April 14 effective date.

Congress should be looking at filling in the gaps in privacy protection, because even if this rule were put into effect, it does not cover all entities that handle an individual's health information and it does not have effective enforcement mechanisms. So we should be moving forward with steps, instead of looking for ways to delay or weaken this regulation.

Let's be clear about this. While almost every Member of Congress pays lip service to the importance of privacy of medical records, over a period of 20 years we have shown that we were uniquely unable to enact detailed legislation. That is precisely why the Congress gave authority to the Department of Health and Human Services to issue a rule if we have failed once again to act.

HHS has now done that. This medical privacy rule is the product not only of many prior years of deliberation by Congress but extensive public involvement as well. In fact, HHS received and considered over 52,000 comments. There is no excuse to delay any further.

Mr. BILIRAKIS. Would the gentleman please summarize?

Mr. WAXMAN. I will, Mr. Chairman. I just want to say that if we do not have privacy protections in place, we are going to continue to see 1 out of every 6 American adults take counterproductive steps, such as giving inaccurate information to their physicians or avoiding health care altogether, because of privacy fears.

And Americans are avoiding genetic testing because of concerns about privacy and discrimination. I think some of the arguments that have been used by the industry groups that are fighting this have been almost laughable. They talk about things they would like to do, like build news walls and so forth, even though the rule says take reasonable efforts.

Mr. BILIRAKIS. With all due——

Mr. WAXMAN. Mr. Chairman, I want to close my comments by saying when these rules were pending, the Department of Health and Human Services went to the Ways and Means Committee and sent a representative to talk about this issue. They did not have to stay away from commenting before the Congress because a rule was pending. I don't think Secretary Thompson should stay away from Congress and use that as an excuse because a rule is pending. We should be working with them.

[The prepared statement of Hon. Henry A. Waxman follows:]

PREPARED STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Last December, the Clinton Administration issued a medical privacy rule that provides essential protections for American families. The rule is a long-overdue and welcome step toward establishing privacy rules that ensure the effective operation of our health care system.

We should be moving forward to put this rule into effect and build on the solid foundation of privacy protections it establishes. Unfortunately, we are now going in the wrong direction. This situation is accurately described in the title of Tuesday's *USA Today* editorial: "Bogus Scare Tactics Delay Medical Privacy Reforms." Well-

funded interest groups are engaged in concerted efforts to unravel or put off altogether the privacy protections in the rule.

The Administration should be focused on working with affected parties to answer questions and issue any guidance necessary to ensure effective implementation of the rule. Instead, Secretary Thompson re-opened the rule for comment, raising the possibility that implementation of the rule will be delayed beyond the April 14 effective date.

Congress should be focused on filling the remaining gaps in privacy protection. For example, we should be strengthening the regulation by covering all entities that handle an individual's health information, and augmenting the law's enforcement mechanisms. We should move forward with such steps instead of looking for ways to delay or weaken the regulation.

Let's be clear about this. While almost every Member of Congress pays lip service to the importance of privacy of medical records, over a period of over 20 years, we have shown that we are uniquely unable to enact detailed legislation. That is precisely why we gave the authority to HHS to issue a rule if we failed once again to act. HHS has now done that.

This medical privacy rule is the product not only of many prior years of deliberation by the Congress but extensive public involvement as well. In fact, HHS received and considered over 52,000 comments. There is no excuse to delay further.

The current absence of privacy protection is not without consequences. A recent survey showed that one out of every six American adults takes counterproductive steps, such as giving inaccurate information to their physicians or avoiding health care altogether, because of privacy fears. Other studies show that Americans are avoiding genetic testing because of concerns about privacy and discrimination.

Increased confidence in health privacy protections will mean that more American consumers will be willing to seek out health care that could prevent or result in early screening of conditions that are significantly more costly to treat at later stages.

I believe that policymakers should carefully examine the various questions that have been raised regarding the rule. But I have heard no good argument for delaying the rule during this process.

And as we go through this process, I urge that we avoid indulging silly hypothetical scenarios that spread misinformation about the rule. We've heard a lot of these in recent weeks.

For example, as pointed out by the *USA Today* editorial, the rule requires "reasonable" safeguards to prevent inappropriate disclosures. Yet some are claiming this means "hospitals might have to build soundproof walls between patients in recovery rooms." The rule also requires "reasonable efforts" to limit the disclosure of a patient's health record to the minimum amount necessary. Yet at a recent industry briefing for congressional staff, one speaker claimed this means covered entities might have to "clip a microphone on every employee to record what he or she says so we could audit that information." These kinds of comments are difficult to take seriously.

I hope that this hearing provides for a productive discussion of medical privacy issues. Given that there are pressing questions regarding why Secretary Thompson opened up the rule for additional comment and what his intentions are regarding implementation, it would have made sense for the majority to ask the Secretary to testify at this hearing. I want to note that I'm disappointed that this invitation was not extended.

That said, I look forward to hearing from the witnesses who are before us today.

Mr. BILIRAKIS. The gentleman's time has expired. Secretary Thompson will appear before this committee or the full committee, whatever the case may be, and respond regarding their position on these regulations.

Dr. Norwood.

Mr. NORWOOD. Thank you very much, Mr. Chairman. I do appreciate you holding this hearing. A few weeks ago the House took up consideration of the regulations on ergonomics. Many of us felt that the regulation on ergonomics was ill conceived and would have led to a tremendous disruption in a range of industries. It did not mean we do not believe that there is such a thing as repetitive motion syndrome. We did not believe that rule, that regulation was

correct. We feel strongly that those regulations were the wrong thing to do, and Congress voted to rescind the regulations.

So here we are this morning, considering another rule with the potential to have a tremendous impact on a wide range of industries in the health care system. While I do not have feelings about medical records privacy as strongly as I do about ergonomics, I feel that we do not fully understand yet the potential negative impact that privacy regulations can actually have on health care; and, thus, an important hearing this morning, hearing from people who are involved in it.

I hear the concerns many of our witnesses have expressed in their testimony and I share some of those concerns. We may not know just how extensive the difficulty in complying with and implementing the privacy regulations are until the health care system tries to meet them. Then we may find ourselves back here considering a revision or even rescinding those rules. I hope that is not the case.

Let's be clear about this. We all know how important medical privacy is, but it is equally important to do the rules and regulations in a correct way so that we avoid as many of the pitfalls as we possibly can.

I thank you again for having this hearing and look forward to hearing our witnesses and thank them for being here.

Mr. BILIRAKIS. I thank the gentleman.

Mr. Dingell, for an opening statement.

Mr. DINGELL. Mr. Chairman, thank you. First of all, I commend you for holding this hearing. Second of all, I applaud your announcement that we will hear from the Secretary prior to the Easter recess. I think that is very much in the public interest.

Mr. BILIRAKIS. Every effort is being made toward that end, sir. We have not had a 100 percent assurance. That is certainly our goal, and they know that.

Mr. DINGELL. I certainly commend you for that. I hope it will be the strong position of this subcommittee and this committee that until the Secretary has had an opportunity to explain these matters to the committee in great detail, that we will expect that the rule or the regulation will not be set aside.

I would observe to you, Mr. Chairman, that the story of Pandora's box provides to us a useful analogy to the situation in which we find ourselves. When a person's medical privacy is taken from them and their personal information is made available for use against them, then that person is irretrievably injured. I would point out that there is no hope whatsoever that once a person's medical information is released and put into the marketplace, that there is no hope that that person has that it will not be used against him in connection with employment, in connection with purchase of large capital items, homes, refrigerators, things of that kind, or in connection with retirement or insurance or any other economic question which might affect that individual, including, I would note again, his job.

So I think it is extremely important that if there is to be error on this matter, that that error occur on the side of protecting the privacy of an individual. Americans constantly come to me and talk to me about protection of their privacy, their family's privacy, their

concerns about their medical privacy, and there are a large number of people who constantly feel that there are people out there spying on them. It isn't necessary to spy on people. All you do is go to the records, and the records are abundant, and it is very easy to get the information without tapping telephones or things of that kind.

I can no longer tell American people that their personal records or their personal information, medical, financial, or other, are adequately protected and that they are safe in their personal privacy. And I have regrets about that, because that is been a very important component of being an American.

I have a long statement which I would put in the record. I will conclude Mr. Chairman, by pointing out Americans distrust the system, Americans are going and paying out of their own pocket for medical care rather than utilize something which may finance their medical care, but which might generate information which can be used against them. This is a serious matter and Americans should be able to have greater confidence in the system than they have now.

I know, Mr. Bilirakis, Mr. Chairman, you will keep your word and we will hear from HHS before the April break. I would observe that if the Secretary puts these matters that he has discussed with regard to this regulation into play and into motion prior to the time he has been heard before this committee, I will regard it as a breach of faith on his part and as an unfriendly act, not just to me and to this committee, but also to each and every American who is concerned about his or her medical privacy. And I will view it as another example of this administration rushing to undo a large number of regulations and steps which were taken that would protect the interests of the American people with regard to health, with regard to personal privacy, with regard to protection of the environment and other matters. And I simply observe this, Mr. Secretary: We will keep an eye on you and you will be judged by what you are doing on this particular matter.

Thank you Mr. Chairman.

[The prepared statement of Hon. John D. Dingell follows:]

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

Mr. Chairman, the subject of this hearing is one of importance to every American. According to a 1999 study by Princeton Research Associates, one in six Americans has done something out of the ordinary to keep personal medical information confidential. Improper disclosure of medical information can result in embarrassment, discrimination, and denial of proper health care. According to another survey by Louis Harris & Associates, twenty-seven percent of those polled believed their medical information had been improperly disclosed. Eleven percent of consumers polled said they or a family member paid out-of-pocket for health care in order to protect their privacy.

There's more. One survey estimated that seven percent of consumers chose not to seek care because they did not want to jeopardize their job prospects or other life opportunities. Sixty-three percent of respondents in another survey said they would not take genetic tests for diseases if insurers or employers could obtain the test result.

We will hear some complaints about the regulation today, but I want to remind everyone that this rule provides important safeguards for people's health. I am not aware of any organization representing persons whose medical information would be protected by this rule that has urged a delay in the implementation of this regulation. Indeed, many providers support the regulation and support its implementation.

I am pleased that we will hear from the American Nurses Association. Nurses are the front line of our health care system. They are overworked. The nursing profession faces crucial recruitment and retention problems. If this regulation presented some undue burden, or was vague, I think the nurses would tell us. What they will tell us is that health care suffers without strong privacy protections.

We will also hear from the American Psychiatric Association. Each year, an estimated 56 million Americans—one in five people—experience diagnosable mental disorders. Too much of this goes untreated. Why? Effective psychotherapy depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. Because of the sensitive nature of the problems for which individuals may consult a psychotherapist, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason, the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment.

Each profession that provides mental health treatment embraces confidentiality as a core ethical principle. Confidentiality generally is considered to be a cornerstone of a doctor-patient relationship. Therefore, the basic requirements of the regulation are not new.

Changes in the health care industry and advances in technology present a complex environment in which to implement the regulation. The regulation is characterized by a rule of reason and flexibility. Many of the concerns raised today are based on worst-case, but unrealistic, scenarios. Simple common-sense implementation should resolve these matters.

Where we go from here depends upon the Secretary. He has, unwisely in my judgment, reopened this matter for comment. Moreover, I note that no witness from the Department of Health and Human Services is before us today. I take Chairman Bilirakis at his word that we will hear from HHS before the April break.

Mr. BILIRAKIS. I appreciate the gentleman's remarks. I would reiterate what I said earlier, and that is we have said to the Secretary we want him here. We are going to do everything we can to get him here before the April break. But I don't want to mislead the gentleman that we have 100 percent assurance that he will be here. But you do have 100 percent assurance that that is what we intend and that intention has gotten to and will continue to get to the Secretary.

Mr. DINGELL. Mr. Chairman, if you would yield to me, I would observe that I respect you, I view you as an honorable man and as a capable chairman. The minority stands ready to assist you in assuring the cooperation of the Secretary, and we will show you a number of things that we have found in times past to be useful in assuring the presence of Secretaries who might have otherwise some more recalcitrant approach to the business before us. I also will assure you that we will seek to raise the pain level for the Secretary if he does not wish to cooperate in this matter.

Mr. BILIRAKIS. That having been said, we will continue to do what we intend to do here today, and that is to learn as much as we can about this subject.

Mr. BILIRAKIS. The Chair recognizes Mr. Upton.

Mr. UPTON. Thank you, Mr. Chairman. I will submit my full statement for the record.

Mr. BILIRAKIS. I might add that the opening statement of all members will be made part of the record, without objection.

Mr. UPTON. Thank you. I would just note that I am behind your efforts to get Secretary Thompson to testify on this very important issue before the April break. It might also be somewhat revealing to have now Florida resident and former Secretary Shalala come as well. That might be appropriate. I would just like to note that as I have talked to a number of providers and folks back in my dis-

trict, this is a very important issue. I look forward to the testimony and would like to submit comments from one of my administrators back home as part of my statement as well, and I yield back the balance of my time.

Mr. BILIRAKIS. Without objection, that is the case.

[The prepared statement of Hon. Fred Upton and the information referred to follow:]

PREPARED STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Thank you, Mr. Chairman, for holding today's hearing on the medical records privacy regulation mandated under the Health Insurance Portability and Accountability Act (HIPAA). I am sure that all of us here today would agree that our first priority is the best interests of patients. But since the final regulation was issued last December, I have heard from a number of health care providers in my district who, while not questioning and in fact sharing the good intent behind the regulation, have raised serious concerns about the practical effects of the regulation on their ability to provide timely, coordinated acute and preventive care to their patients.

Last month, in fact, the two largest hospitals in my district gave me a fascinating demonstration of their telehealth/telemedicine systems work to improve the quality, coordination, and continuity of patient care. It's clear that the electronic medical record and beside hospital chart are the future of health care in this country as our basic telecommunications infrastructure expands to bring 21st century medicine into even isolated rural communities. The need for patient protections in this brave new world are clear and pressing, but we must ensure that we "first do no harm" as we structure and implement these protections.

PREPARED STATEMENT OF JAMES B. FALAHEE, JR., VICE PRESIDENT, LEGAL & LEGISLATIVE RELATIONS, BRONSON HEALTHCARE GROUP, INC.

Bronson Healthcare Group ("Bronson") is a medium sized health care system located in Southwestern Michigan, in the Congressional District so ably served by Congressman Fred Upton. Unlike some other health care systems, Bronson consists not only of hospitals, but also employed providers and two health plans. As such, Bronson is impacted by almost every element of the HIPAA regulations.

Bronson, like other health care providers, fully supports privacy rights and recognizes their importance. There already exists an extensive body of case law and statutory authority which currently protects personal privacy rights and has developed over time. The new HIPAA regulations, in Bronson's opinion, are an unnecessary layering of very complicated and confusing regulations on top of the already existing, and working, statutes and case law.

Section 164.530(c)(1) of the new HIPAA regulations provides that a covered entity must "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The Department of Health & Human Services could have confined its entire HIPAA regulations to this one statement and left it at that. Bronson submits that it, and other covered entities, *already* have in place appropriate administrative, technical, and physical safeguards to protect privacy of protected health information. HHS need not have so intrusively interfered with the current safeguards. The complex and prescriptive regulatory system created by HIPAA is unworkable and not needed.

Bronson has a number of specific issues concerning HIPAA:

1. HIPAA does not supersede state law. Any health care provider or health plan which operates in multiple states must determine whether the laws in the individual states in which it operates are more restrictive than HIPAA. If so, providers need to customize their consents, authorizations, and documents to match the more restrictive provisions of a state's law. This will necessarily lead to a patchwork of different privacy laws, depending on in which state you live. Instead of such a patchwork, if HIPAA is retained, the HIPAA regulations should be revised to include a federal preemption standard.
2. Bronson owns an indemnity insurance company and an HMO. We are concerned as to whether all health plans will be ready for HIPAA implementation and the transactions and code sets which go along with it. If all health plans do not

comply with the HIPAA requirements, the desired streamlining of the payment processes will not be accomplished. We are also concerned that some plans may go beyond HIPAA and require even more information than the standardized transactions/code sets would require. This would defeat the uniformity goal of HIPAA.

3. The HIPAA regulations require that only the minimum necessary personal health information be disclosed. This is an unworkable requirement. Each time information is requested or discussed, a health provider or covered entity must now determine if the "minimum necessary" standard is met. This could present a risk to patients if vital treatment information is delayed or denied.
4. The HIPAA regulations will place an onerous burden on individual physician providers and, even more so, on patients. The primary goal of the health care community should be to deliver high quality patient care. Bronson is concerned that the HIPAA regulations will interfere with the delivery of such care. For example, upon admission to its facilities or its physicians' offices, Bronson will now be required to give each patient (or patient representative) forms, notices, and requests for authorization which will be, at a minimum, 10 pages long. We question whether these forms, notices, and authorizations will be read and, if read, will be understood by patients, their families, or authorized representatives.
5. The exhaustive HIPAA regulations are yet another unfunded mandate on the health care community. Bronson has not yet been able to calculate its cost of implementation, but knows it will require hundreds of hours of training and education, and the review and revision of over 800 contracts with vendors and suppliers.

Bronson recommends that the Department of Health & Human Services develop new, more streamlined regulations which address these and other comments raised by those in the field. Bronson strongly recommends that HHS meet with health care providers prior to formally responding to the comments it receives during March, 2001. A series of meetings between HHS, providers, and privacy advocates will go a long way to mitigating the backlash which has occurred as a result of the December, 2000 HIPAA regulations. Bronson would be more than willing to participate in such meetings.

Thank you for the opportunity to submit these comments. Bronson would be glad to work with HHS and this committee to assure that personal health information is protected, but that high quality patient care is not adversely impacted by such privacy protections.

Mr. BILIRAKIS. Ms. Capps.

Ms. CAPPS. Thank you, Mr. Chairman, for holding this hearing. It is so important that this committee hear the testimony, because the debates revolving around medical privacy and the role of the Federal Government are central, I believe, to the very issue of access to care. The single most important factor in providing quality care and encouraging people to use it is trust. Patients must be able to trust their health care providers, to trust them to make the right decisions, to pay attention to their interests, to keep the particulars of their cases and lives in confidence. If this trust breaks down, then people will avoid seeking medical attention until they have no choice, and by then the options will be limited and the costs excessive.

This committee has an obligation to the American people to protect that trust and to protect the rights of our constituents. And this is why a Patient's Bill of Rights is so important and this is why adequate privacy regulations need to be put in place.

As we examine the proposed privacy regulations, I hope that each member of this committee will remember that what is at stake here is not the work of one administration or another, what is at stake is the very confidence that Americans have in their doctors, nurses, hospitals, health centers and other health care providers; that they be focused on treating their needs and not exploiting their weaknesses.

By and large, most health care providers have a very good track record of protecting patients' privacy. Doctors and nurses are rigorously trained to be cautious with a patient's personal information. But we need to make sure that the pressures of the financial bottom line do not tread on this critical right. On the other hand, we also need to avoid discouraging medical research and overcomplicating our health care system. New, creative innovations can be essential to providing the best care possible and they are dependent on information about current medical conditions.

I don't believe these goals have to be in conflict. I think it is possible to protect the rights of patients while enabling proper medical research, and this should certainly be our objective. I believe that the current proposed regulation is a good step in the right direction. Many of the concerns about the regulation can hopefully be resolved from guidance of the Department of Health and Human Services. I certainly hope that neither this committee nor the administration will do anything that will weaken the protections for patient privacy.

I look forward to hearing what my colleagues and the panelists have to say about these regulations.

I want to particularly recognize Ms. Mary Foley, the President of the American Nurses Associations. I am pleased she is here with us to share the views of the nursing community. As a nurse myself, I understand how important it is to include perspectives of nurses on these issues. Nurses are the first line of defense on health care matters and we need to make sure that our voices are heard in the hearings and meetings with policymakers. I have tried to do this in my stay in Congress and I am glad to see that the ANA is here to do that now. I commend your efforts and I am interested in your views on what we should do.

Mr. Chairman, I thank you for holding this hearing, I look forward to working with you on this issue. And I know we will strive together to do this in a bipartisan way.

Mr. BILIRAKIS. I thank the gentlelady for her statement.

Dr. Ganske for an opening statement.

Mr. GANSKE. Thank you, Mr. Chairman. We are here today because Congress couldn't reach an agreement on the medical record privacy regulations. So at Congress' direction, the previous administration gave the Department of Health and Human Services the job of creating new rules. The complexity of the result reflects the complexity of the problems we face.

In crafting rules for the health care industry, courts, banks and insurers, HHS attempted to balance the conflicting demands for privacy and productivity. Initially the rules covered only information maintained or transmitted electronically. Not good enough, critics shouted. So HHS extended the rules to paper files and information transmitted orally. Too far, shouted different critics.

HHS received over 52,000 comments on its privacy rules. What they found was that outlawing hacking and malevolent use of personal information is simple. Enforcing those bans is hard. In each instance, they found they had produced an exceedingly complex compromise that is assaulted as too loose by privacy advocates and too onerous by industry. Writing rules prohibiting the infringement of privacy without denying doctors and researchers the benefits of

the information technology is difficult. So is drawing lines telling the health care industry what they can share, what they can't, and with whom they can do so. How much should patients know before medical researchers tap into their records? Does it make sense that business can share your personal data with their affiliates?

Conflict between society's need to know and individuals' right to privacy isn't new. As HHS said in December when it tested the rules, quote: "we expect insurers and the government to reduce fraud, we expect to be protected from epidemics, and we expect medical research to produce miracles. We expect the police to apprehend suspects and we expect to pay for our care by credit card.

"all these activities involve the disclosure of health information to someone other than our physician. We have expectations as a society that conflict with individuals' views about the privacy of health information," unquote.

Well, while recognizing that conflict, the implementations of the final rule was delayed by the Bush administration. Mr. Chairman, I note that we don't have today a representative from the hospital community, so with your permission, Mr. Chairman, I would like to introduce a letter into the record from the Iowa Hospital Association regarding the final medical record privacy rule.

Mr. BILIRAKIS. Without objection, that is the case.

[The information referred to follows:]

IOWA HOSPITAL ASSOCIATION
March 16, 2001

The Honorable TOMMY G. THOMPSON
Secretary, U.S. Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, S.W.
Washington, D.C. 20201

DEAR SECRETARY THOMPSON: The Iowa Hospital Association (IHA) is pleased with your recent announcement that you will open a public comment period on the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rules. IHA is a statewide membership services organization that advocates for 116 community hospitals and health systems as well as the patients and communities they serve.

Iowa hospitals and health systems have been proponents of standardization of electronic transactions related to health care and support the administrative simplification provisions of HIPAA. Iowa hospitals and health systems also take very seriously the privacy of the patients and communities they serve and have a long-standing commitment to safeguarding this privacy while delivering high-quality health care to their patients.

The Department of Health and Human Services (HHS) final rule on privacy will have significant impact on the day-to-day operations of Iowa hospitals and health systems. Hospitals and health systems will have to invest substantial resources to comply with this overly complex and pervasive regulation. Iowa hospitals and health systems today face an emerging crisis in workforce shortages and the significant regulatory burden of the HIPAA privacy rules will heighten this crisis. In addition, the lingering financial burdens imposed by the Medicare payment cuts of the Balanced Budget Act (BBA) of 1997 have severely strained the financial resources of our hospitals and health systems.

IHA respectfully requests that HHS suspend the April 14, 2001 effective date and significantly rewrite the HIPAA privacy rules. IHA believes that it is appropriate for your department to reexamine these regulations to ensure that implementation of privacy standards does not hinder the ability of hospitals and health systems to deliver high quality health care and does not put hospitals and health systems in further financial jeopardy. There is a balance that must be achieved between delivering cost-effective, quality health care and protecting patient privacy.

We suggest the rule be substituted by a simpler version. In keeping with the original intent of the legislation—to streamline health care administration—the rule

should focus on the potential misuse of information by employers and health insurers. Consent should be required only for such non-medical use.

The following are comments and recommendations of IHA on the final privacy rules.

GENERAL COMMENTS

The final privacy rule threatens the balance between the cost-effective delivery of high quality care and patient privacy in a number of ways:

Scope

The Department of Health and Human Services' authorization to adopt privacy rules under HIPAA is limited. Under the act, confidentiality regulations are to apply only to electronic transactions and the data elements for such transactions, and to assure the privacy of health information exchanged electronically. The final privacy rule applies privacy standards to all uses and disclosures of protected health infonnation—electronic, written, and oral—far exceeding the Department of Health and Human Services' statutory authority. The result is a regulation that:

- Is so complex that it is extremely difficult, if not impossible to determine how to achieve efficient compliance.
- Creates significant barriers to current treatment and quality improvement activities.
- Conflicts with the clear cost-savings intent of the administrative simplification section of HIPAA.

Costs

The Department of Health and Human Services needs to analyze and assess how compliance with the privacy rule will impact the cost of caring for patients. The estimated cost impact of the final privacy rule on hospitals and health systems needs to be calculated and weighed against the benefits of the rule. The American Hospital Association has estimated that the total cost to hospitals and health systems complying with the final privacy regulations will be up to $22.5 billion over five years.

The Department of Health and Human Services must recognize the tremendous burden placed on health care providers who are now facing simultaneous implementation of multiple, complex federal and state regulations. Hospitals and health systems over the last few years have had to address Y2K system problems, make significant changes to their patient data collection, coding and billing systems to implement prospective payment systems for Medicare skilled nursing care, home health care, and outpatient care, in addition to facing changes to a variety of other regulations significantly impacting their day-to-day operations.

In addition, Iowa hospitals and health systems face critical shortages in nursing and in personnel in other clinical areas. The staffing issues associated with implementing the privacy regulations need to be considered. Implementation of the privacy rule as published will further add to providers' already overwhelmed administrative and information systems and represents yet another unfunded mandate.

Implementation Schedule

The final privacy rule requires all health care providers to implement the privacy standards two years after their effective date. Since the regulations are extremely complex and extensive, this schedule is not practical.

Further, serious consideration should be given to coordination of the privacy rule implementation deadlines with the implementation deadlines of the other HIPAA regulations. HIPAA included numerous components affecting privacy, security, and administrative simplification. Not all of the regulations to implement these provisions have been developed. Final implementation of all of these provisions should be synchronized to assure that providers in responding to multiple interrelated regulatory provisions do not incur additional costs. IHA would suggest that implementation of the HIPAA provisions regarding privacy, security, and administrative simplification not occur until at least two years following the promulgation of the final set of relevant regulations.

Preemption

The final regulations fail to preempt conflicting state laws. The American Hospital Association's cost estimates for this provision alone over a five-year period are $372 million. IHA is concerned that state laws that are contrary or more stringent will cause considerable confusion. It is not uncommon for health systems to operate hospitals and other health care facilities in multiple states, to serve patients from other states, and to provide care under arrangements with health plans that serve

populations from several states. Addressing the many different state rules will be extraordinarily difficult for individual providers and will lead to confusion as to what rules apply. The lack of clear preemption complicates the ability for providers to develop clear and consistent privacy policies. Providers must not only comply with multiple state requirements, but now also understand how the federal rules relate to state requirements.

Peer Review Protection

Provisions in the final regulations may threaten peer review protections. Peer review protections are intended to foster a comprehensive, quality system for the effective reduction of medical/health care errors and other factors that contribute to unintended adverse patient outcomes in a health care organization. This environment encourages recognition and acknowledgment of risks to patient safety and medical/health care errors; the initiation of actions to reduce these risks; the internal reporting of what has been found and the actions taken; a focus on processes and systems; and minimization of individual blame or retribution for involvement in a medical/health care error. It encourages organizational learning about medical/health care errors and supports the sharing of that knowledge to effect behavioral changes in itself and other health care organizations to improve patient safety. The final regulations should be reviewed to make sure that notice and authorization provisions do not hinder the development of internal safety reporting and quality improvement initiatives.

Notice, Consent, and Authorization

Notice and consent requirements added to the final rule will significantly complicate compliance efforts and activities. These components represent a significant departure from the proposed regulations in that the final privacy rules require a consent for uses and disclosures of protected health information for purposes of treatment, payment, and health care operations. A separate authorization to use and disclose protected health information for "other purposes" must be obtained separately from the consent. The terms "consent" and "authorization" do not overlap and differ substantially in their content. Notices regarding privacy must be added to such things as appointment reminders. All of these requirements add administrative costs with little or no benefit to patients. Hospitals and health systems are already required by both federal and state governments to post numerous notices and to provide written notice of various rights and responsibilities. Instead of requiring yet more notices and more paperwork, the regulations should allow hospitals and health systems to incorporate appropriate notification regarding privacy into existing notices and patient rights' materials.

Minimum Necessary Disclosure

While the final privacy rule tempered the "minimum necessary disclosure" limitation among health care providers, it continues to pose a significant and costly barrier to compliance with the privacy rule. This standard is ill-defined in the privacy rule and will likely result in numerous and varied interpretations. Hospitals and health systems are required to develop criteria to limit the amount of information disclosed and to evaluate each and every disclosure against these criteria. Hospitals and health systems are required to train all employees regarding these criteria and to establish a "privacy officer" to ensure responsible implementation. Again, these specific requirements impose significant personnel requirements and administrative costs, and redirects a caregivers time away from patient care.

Business Associates

In the final privacy rule, the Department of Health and Human Services is holding covered entities responsible for the protection of personal health information by their business associates. The legal work and costs associated with implementing this provision will be overwhelming. Hospitals and health systems will have to renegotiate contract provisions that ensure that these business associates protect the information that is released to them in the normal course of health care operations. It would be more appropriate if the regulations held all parties accountable for their own improper disclosure of personal health information. Hospitals and health systems should not be responsible for the improper disclosure of personal health information by other organizations.

Quality Improvement & Statewide Data Collection Efforts

Centralized data collection activities both by state hospital associations or state government intended to produce comparative incidence rates, patient outcome measures, and utilization and cost data heavily utilized by management in hospitals and health systems, are threatened by the privacy rules as written. Further, the inclu-

sion of patient county and zip code as protected health information may limit the ability to use discharge data for quality improvement and community health surveillance activities. These activities are important to hospitals and health. systems that seek to develop integrated services in response to patient and community health needs.

RECOMMENDATIONS

As published, the final privacy rules are unworkable and will cost the health care community billions of dollars to attempt compliance at a time when hospitals and health systems are experiencing severely restricted resources, both capital and workforce. The costs of implementing the final privacy rules far outweigh any potential long-term savings through administrative simplification. The rule also requires an unrealistic timeframe for implementation and has not been coordinated with the related HIPAA rules affecting security and administrative simplification. Therefore, IHA recommends the following steps be taken to reform the new privacy rule in a manner that safeguards both patient privacy and patient care.

1. Suspend the final privacy rule prior to its April 14, 2001, effective date.
2. The Department of Health and Human Services should consult with hospitals and health systems on site at their facilities to discuss the practical implementation issues and problems that have been identified in order to reasonably resolve as many of these issues as possible prior to implementation of the privacy standards. IHA could facilitate Department of Health and Human Services' staff visits to hospitals and health systems within Iowa.
3. The Department of Health and Human Services should appropriately narrow the scope of the regulation to apply privacy standards addressing the subjects outlined in the statute to the individually identifiable health information used in connection with electronic transactions as outlined in the statute.
4. The Department of Health and Human Services should revise the HIPAA regulation implementation schedule according to the following principles:

- No health care provider should be required to begin implementation of HIPAA until all HIPAA privacy, security, and administrative simplification regulations have been finalized.
- A single, uniform date of compliance should be established at least two years after promulgation of all HIPAA final regulations to allow a sufficient and reasonable time period in which to implement.

5. Statewide data collection and use efforts, that have been in operation for years with safeguards taken to protect health information, should be provided safe harbor in the final privacy regulations.

Again, we are pleased that you are allowing for public comment on the final privacy rules and are hopeful that this first step will lead to fundamental reform of the privacy rules. IHA is committed to working with HHS to develop privacy rules that not only safeguard patient privacy, but also ensure delivery of cost-effective, quality patient care. Please contact Perry Meyer, Tracy Warner or Maureen Hockmuth at IHA at 515/288-1955 if you have any questions.

Sincerely,

STEPHEN F. BRENTON
President

cc: Iowa Congressional Delegation

Mr. BILIRAKIS. And at the same time I would ask unanimous consent that I might introduce a letter from the Florida Hospital Association, as well as statements and written testimony from the American Council of Life Insurance, and from the Health Insurance Portability Biotechnology Industry Organization. Without objection, that would be the case.

[The information referred to follows:]

FLORIDA HOSPITAL ASSOCIATION
March 16,2001

The Honorable MICHAEL BILIRAKIS
Room 2269 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

DEAR REPRESENTATIVE BILIRAKIS: The Florida Hospital Association, which represents 230 not-for-profit, investor-owned and government hospitals and health Systems, seeks your help in an urgent and time-sensitive matter. We ask that you con-

tact Health and Human Services Secretary Tommy Thompson to request that he delay the April 14, 2001, effective date of the privacy rules promulgated under the Health Care Portability and Accountability Act (HIPAA). FHA members are deeply concerned about the regulation and request that you join with us and ask the Secretary to fix the rule.

Florida's hospitals are committed to safeguarding the Privacy of patients' medical information. However, we are extremely concerned about the effect the final HIPAA medical privacy rules will have on hospitals. The rules are so complex and prescriptive in many areas that they will be both unworkable and unreasonably costly. The rules were reopened for public comment on March 1, 2001. HHS must receive your request no later than March 30, 2001. Time is short.

We believe that patients have the right to every consideration of privacy, including the right to review and understand their medical records. However, in their current form the HIPAA privacy rules are so complex and prescriptive that they are both unworkable and excessively costly. They will hinder the ability of providers and families of patients to coordinate the care for patients.

Florida's hospitals need your help: Please ask HHS to delay the rules and fix them.

Sincerely,

CHARLES F. PIERCE, JR.
President, FHA Orlando

PREPARED STATEMENT OF THE AMERICAN COUNCIL OF LIFE INSURERS

This testimony on Assessing HIPAA: How Federal Medical Privacy Regulations Can Be Improved is submitted to the House Commerce Subcommittee on Health on behalf of the American Council of Life Insurers (the ACLI). The 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 73 percent of the companies that provide disability income insurance. The ACLI appreciates the opportunity to submit this statement.

The ACLI strongly supports the underlying goal of the Standards for Privacy of Individually Identifiable Health Information (the Regulation) issued by the Department of Health and Human Services (the Department)—protecting individually identifiable health information. Life, disability income, and long term care insurers understand their responsibility to protect their customers' 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 this information. Several years ago, the ACLI Board of Directors adopted the "Confidentiality of Medical Information Principles of Support." These Principles were recently strengthened providing ACLI support for prohibitions on the sharing of medical information for marketing and for determining eligibility for credit. (A copy of the Principles is attached.)

The ACLI believes that the Regulation's goal of protecting individually identifiable health information may be achieved in a manner consistent with the significant public interest in maintaining the life, disability income, and long term care insurance markets which meet the private insurance needs of millions of American consumers. By their very nature, the businesses of life, disability income, and long term care insurance involve personal and confidential relationships. However, insurers selling these lines of coverage must be able to obtain and use their customers' health information in order to perform legitimate insurance business functions, such as underwriting and claims evaluation. The performance of these functions is essential to insurers' ability to serve and fulfill their contractual obligations to their existing and prospective customers.

The Regulation will have a significant and direct impact on the manner in which life, disability income, and long term care insurers do business. Although life and disability income insurers are not "covered entities" under the Regulation, their ability to obtain individually identifiable health information will be subject to the Regulation's disclosure requirements and limitations. This is true because life and disability income insurers often must obtain individually identifiable health information from health care providers which are "covered entities" under the Regulation. Covered entities may only disclose protected health information as permitted under the Regulation.

Long term care insurers are covered entities under the Regulation. As such, they are subject to the full ambit of the Regulation's requirements regarding access, use and disclosure of individually identifiable health information. In addition, like life

and disability income insurers, long term care insurers' ability to obtain individually identifiable health information from other covered entities (health care providers) is subject to the Regulation's disclosure limitations and requirements.

A number of changes were made in the final Regulation in response to concerns raised by the ACLI in connection with the proposed regulation's disclosure requirements. However, there continue to be ambiguities in some provisions of the final Regulation which could be construed to limit covered entities' disclosure of individually identifiable health information to life, disability income, and long term care insurers. This would limit these insurers' access to and use of health information critical to their ability to perform fundamental insurance business functions, such as underwriting and claims evaluations.

Below are more detailed explanations of the manner in which life, disability income, and long term care insurers use protected health information and ambiguities in the Regulation which could be construed to jeopardize legitimate and essential uses of that information by life, disability income, and long term care insurers.

WAYS IN WHICH LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURERS USE INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

The process of risk classification is a system of classifying proposed insureds by level of risk. 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 risks pay the same premiums. 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 administra-

tion of 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 Medial 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 cost of which is ultimately borne by consumers.

AMBIGUITIES RAISED BY THE FINAL REGULATION

The following summarizes ACLI member companies' major concerns with the Regulation listed in order of their importance. As indicated above, ACLI member companies' most fundamental and critical concerns relate to the Regulation's likely significant and adverse impact on their ability *to obtain* protected health information, critical to the business of insurance, from health care providers.

ACLI member companies are very concerned by a number of ambiguities in relation to the *minimum necessary standard* set forth in *Sections 164.502(b)* and *164.514(d).* Medical underwriting on the basis of individually identifiable health information lies at the core of the present systems of life, disability income, and long term care insurance. In order for insurers to be able to fairly and prudently underwrite, they must be able to access and use protected health information relevant to the proposed insured's likelihood of dying prematurely, becoming disabled, or requiring long term care. Insurers must also be able to access protected health information to pay claims for benefits submitted under existing life, disability income, and long term care insurance policies.

Life and disability income insurers are concerned by *Sections 164.502(b)(1)* and *164.514(d)(3)* which would require a covered entity to only disclose the minimum amount of information which *it* believes to be necessary to accomplish the purpose for which the information is requested. It does not appear to be the intent of the drafters of the Regulation, nor would it make practical sense, to subject to this standard disclosures of protected health information made pursuant to the authorization of the individual, the type of authorization used by life and disability income insurers. However, because this is not entirely clear, life and disability income insurers are concerned that covered entity health care providers will construe the minimum necessary rule to require them to disclose as little information as possible to life and disability income insurers. As a result, life and disability income insurers are likely to be denied access to information essential to their ability to make fair and prudent underwriting decisions and appropriate claims evaluations, among other things.

Long term care insurers are also concerned by the *minimum necessary requirements* of *Sections 164.502(b)* and *164.514(d).* They are particularly concerned that the language of *Section 164.502(b)(2)(ii)* may be construed by covered entity health care providers to subject disclosures of protected health information to covered entity long term care insurers to the minimum necessary standard. Like life and disability income insurers, long term care insurers strongly believe that health care providers are not in a position to know what information is needed to underwrite an application for insurance coverage or to evaluate a claim; nor does the health care provider bear the financial risk of issuance of an insurance policy.

Long term care insurers are also concerned that under Section 164.504(d), they may only *request* the *minimum amount of information necessary* to accomplish the

purpose for which the information is requested. At the inception of the underwriting process for a long term care insurance policy, it is generally impossible for a long term care insurer to know what information may be in a proposed insured's medical record that may be relevant to the individual's likelihood of requiring long term care in the future. Until the long term care insurer sees the individual's *entire medical file,* it often does not know what is the minimum amount of information necessary to underwrite an application for coverage. Unfortunately, the Regulation is very unclear as to how its requirements in relation to the minimum necessary standard will interface with the requirements governing covered entities' right to use and disclose an individual's *entire medical record.*

Concerns of life and disability income insurers, as well as long term care insurers, in relation to the minimum necessary requirements, are exacerbated by the lack of clarity in *Section 164.514(d)(5)* permitting a covered entity to disclose, use, and request an individual's *entire medical record.* They are concerned by the ambiguity as to the intended interplay between this provision and those provisions articulating the minimum necessary standard.

The nature and level of justification required for a disclosure or use of an entire medical file to be "specifically justified" is unclear. Moreover, at the inception of the underwriting process, it is impossible for the insurer to know what information is in the individual's medical file that is likely to be material to the individual dying prematurely, becoming disabled, or requiring long term care. Finally, there is no practical reason why an individual should not be able to authorize the use or disclosure of his or her entire medical record and why that authorization should not appropriately govern the actions of the covered entity.

Section 164.514(d) should be clarified to provide that an authorization for use or disclosure of an entire medical file is "specifically justified" if it is submitted in connection with the underwriting of an application for insurance coverage or evaluation of a claim for insurance benefits. It should also be made clear that under these circumstances, the authorization for use or disclosure of the entire medical file takes precedence over any requirements in relation to the minimum necessary standard.

Life, disability income, and long term care insurers are very concerned that ambiguity in the language of *Section 164.522,* relating to *agreements to restrict use and disclosure of information,* will also have a "chilling effect" on doctors' and hospitals' disclosure of protected health information to life, disability income, and long term care insurers. They believe that if this section is not clarified, it may be construed to permit and uphold agreements to withhold protected health information which is material to underwriting and claims evaluations by life, disability income, and long term care insurers. Since there is no requirement that the covered entity provide notice to the effect that information is being withheld pursuant to such an agreement, the insurer receiving other protected health information from the health care provider is likely not to know that the restricted information existed in the first place or that any information is being withheld. If this practice were to become widespread, it could cause adverse selection. It could significantly undermine the underwriting and claims processes, jeopardizing the current private systems of life, disability income, and long term care insurance. It would legalize actions which constitute fraud and material misrepresentation under current law.

Although the actual words of the Regulation only require covered entities to permit an individual to request restriction of the use or disclosure of protected health information *to carry out treatment, payment, and health care operations,* insurers are concerned that health care providers that enter into such agreements will treat disclosures to life, disability income, and long term care insurers no differently from uses or disclosures for purposes of treatment, payment, or health care operations. This concern is exacerbated by the fact that disclosures to life, disability income, and long term care insurers are not included in the list of situations under which agreements to restrict are not effective set forth in Section 164.522(a)(1)(v). Furthermore, ACLI member companies are very concerned by this section of the Regulation's clear sanctioning of segregation of certain parts of individuals' medical records.

ACLI member companies have a number of concerns in relation to the *authorization requirements* set forth in *Section 164.508.* They are concerned by the *level of specificity* required in authorization forms by *Section 164.508(c)(i)* which prescribes that the information to be used or disclosed be identified in a "... specific and meaningful fashion." As discussed above, is it generally impossible for life, disability income, and long term care insurers to know "up front" what information in an individual's medical record they may need to underwrite appropriately. Moreover, this degree of specificity gives rise to concern that insurers will have to "tailor" authorization forms for each individual in order to obtain necessary underwriting and claims information. This would be very expensive.

Life, disability income, and long term care insurers have grave concern with the Regulation's provisions relating to an individual's *right to revoke an authorization* set forth in *Section 164.508(b)(5).* Contrary to its apparent intent, *Section 165.508(b)(5)* fails to adequately protect insurers against fraud and material misrepresentation in origination of insurance policies or in the payment of claims. This is true because this section fails to provide life and disability income insurers, which are not covered entities, any protection for having taken action in reliance on an authorization; and it fails to clearly limit individuals' right to revoke authorizations obtained as a condition of obtaining insurance coverage or payment of claims.

ACLI member companies are concerned by the *definition of "psychotherapy notes"* set forth in *Section 164.501* and the limitations on conditioning enrollment and claims payments based on provision of an authorization, articulated in *Section 164.508(b)(4).* Member companies are very concerned that the definition of "psychotherapy notes," for example, does not exclude a "diagnosis", but only excludes a *summary* of diagnosis. *The Best Principles for Health Privacy,* recently published by the Health Privacy Project at Georgetown University states: "The phrase 'psychotherapy notes' includes only the personal notes taken by a mental health professional. The notes do not include diagnostic and treatment information, signs and symptoms, or progress notes, which may be shared in the same manner as other clinical information." Accordingly, the ACLI urges clarification of the definition of psychotherapy notes.

Long term care insurers also are gravely concerned that the definition of "psychotherapy notes," coupled with *Section 164.508(b)'s* prohibition on conditioning enrollment or claims payments on provision of authorization in relation to psychotherapy notes, will result in long term care insurers having to issue coverage and pay claims even if they only receive incomplete information, in relation to the individual's condition. For example, the long term care insurer may only receive a "summary of" the diagnosis, but not the diagnosis.

Long term care insurers are also very concerned by the ambiguity of *Section 164.508(e)* which provides implementation specifications for authorizations requested by a covered entity for disclosures of protected health information by other covered entities. This provision was not in the Regulation as proposed. There is significant concern that it may be construed by covered entities health care providers to inappropriately require a "super" authorization as a prerequisite to disclosure of protected health information to covered entity long term care insurers. It also gives rise to concern because of the reference to it in *Section 164.502(b)(2)(ii)* which could be construed to subject disclosures of protected health information to long term care insurers to the minimum necessary requirement.

The ACLI urges deletion of *Section 164.508(e).* Not only is it beyond the scope of the Regulation as proposed, but it may be inappropriately construed to require special authorizations for disclosure of protected health information to long term care insurers and to inappropriately subject such disclosure of protected health information to long term care insurers to the minimum necessary standard.

Other ACLI member company concerns with the Regulation, include the following:

There is concern that the requirements imposed on "*hybrid entities*" by *Section 164.504(b)* will require member companies to create firewalls, between different divisions of a single company and within single divisions of a company, that will be very difficult to enforce and jeopardize member companies' activities in relation to the detection and prevention of material misrepresentation and fraud in the inception of life, disability income, and long term care insurance contracts.

The rules in relation to *de-identification of protected health information,* set forth in *Section 164.514,* are particularly troublesome to long term care insurers. They are concerned that these rules will jeopardize their ability to perform studies critical to future policy design and experience rating, among other things. There is particular concern with the requirements in *Section 164.514 (b)(2)(i)(B) and (C)* which require removal of specified information concerning geographic subdivisions and elements of dates.

The *definitions of "health care operations" and "payment"* set forth in Section 164.501, are also of significant concern to long term care insurers. These definitions fail to include within their scope fundamental insurance business functions of long term care insurers. Not only will long term care insurers be required to obtain authorizations to use protected health information to perform these basic insurance business activities, but they will be vulnerable to revocation of those authorizations.

Long term care insurers are concerned by the apparent requirement of a written contract in every instance where they disclose protected health information to a business associate working on its behalf. While there is no question that the long term care insurer must always receive assurance that the business associate is safeguarding protected health information disclosed to it by a covered entity, long term

care insurers are hopeful that an exception to the written contract rule may be provided for instances where the risk of improper disclosure is low.

There is concern with *Section 160.203* which provides that "(a) standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provisions of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:. . . (b) The provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E or part 164 of this subchapter." ACLI member companies are concerned about having to make a determination as to which law (state law or the HHS regulation) is "more stringent," and their resulting vulnerability to challenge for their decisions. This is particularly troubling, given that, unlike the proposed regulation, the final Regulation withdrew a provision that would have required HHS to responds to requests for advisory opinions regarding state preemption issues. According to testimony presented to the Senate Health, Education, Labor and Pensions Committee by the United States General Accounting Office, "HHS officials concluded that the volume of requests for such opinions was likely to be so great as to overwhelm the Department's capacity to provide technical assistance in other areas. However, they did not consider it unduly burdensome or unreasonable for entities covered by the regulation to perform this analysis. . ." We are concerned that the Department has determined that it does not have the resources to make determinations on preemption, yet the industry is expected to do so.

CONCLUSION

The ACLI recommends that the Regulation's ambiguities that could be construed to restrict life, disability income and long term care insurers access to and use of protected health information be clarified. ACLI staff will be pleased to respond to any concerns or questions raised by members of the subcommittee.

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.

PREPARED STATEMENT OF THE BIOTECHNOLOGY INDUSTRY ORGANIZATION

The Biotechnology Industry Organization ("BIO") is pleased to have the opportunity to submit testimony expressing our concerns about the federal medical privacy regulation issued under the Health Insurance Portability and Accountability Act of 1996[1] (HIPAA) published on December 28, 2000.[2] BIO represents more than 950 biotechnology companies, academic institutions, state biotechnology centers, and related organizations in all 50 US states and 33 other nations. BIO's members are in the business of conducting and sponsoring research designed to discover medicines, diagnostics, and innovative new forms of therapy. These companies provide a home base for researchers who are committed to finding ways to use science to meet unmet medical needs. For most BIO members, research is their business; only a handful have products approved for marketing. These companies are sustained by their prospective patients' hope and faith in their research enterprise, and by Americans' willingness to invest in that hope.

BIO's long-standing role as a proponent of federal legislation and regulations to safeguard the confidentiality of medical information stems from the recognition that (1) the availability of sensitive and detailed medical information about individuals is indispensable for biomedical research, and (2) this availability depends on patients' trust and confidence that researchers will use medical information responsibly and protect it from misuse. BIO's members have long endorsed the principles of respect for the medical privacy of individual patients and strong laws with incentives for all concerned to protect medical information from abuse and unauthorized disclosure. Researchers work hard to maintain the trust and confidence of the patients who make themselves available for research.

BIO's members also believe, however, that patients are counting on them to vigorously pursue their research objectives. BIO believes that the public interest in the discoveries and findings of research is as strong as the public interest in medical privacy. We note that since the enactment of HIPAA, the public debate and hearing record amply document that no one—from patient groups to privacy advocates, providers, payers, and government officials—advocates that research should be made more difficult or costly by the legal framework that we establish to protect medical privacy.

BIO is pleased that the final regulation published on December 28, 2000 makes some significant improvements over the proposed rule regarding issues critical to the conduct of research. Our purpose in submitting this testimony is to express our great concern that the regulation still imposes significant new administrative burdens on those covered entities that choose to collaborate in our research activities, and we do not believe that these burdens are warranted in the context of the HIPAA administrative simplification regulations. Traditionally, a majority of clinical research sponsored by biotechnology companies involves collection of data by investigators associated with academic medical centers or other institutions that are "covered entities" that are required to comply with the new regulation. BIO is deeply concerned that the additional costs of the significant new administrative requirements, together with the new civil and criminal liability to which they are exposed, may have the unintended consequence of making these institutions reluctant to host sponsored research, or incur greater cost and risk to do so.

In particular, we are concerned that as they scramble to meet the aggressive timetable for bringing their patient care and reimbursement activities into compliance over the next two years, these entities may not have the time and resources to meet the new requirements for research—imposed by the regulation including developing the new forms, implementing the new review criteria and modifying the duties of

---

[1] Pub. L. No. 104-191 (Aug. 21, 1996) (amending the Social Security Act ("SSA") by adding Part C of Title XI, codified at 42 U.S.C. §§ 1320d *et seq.*).

[2] 65 Fed. Reg. 82462 (Dec. 28, 2000).

Institutional Review Boards (IRBs). Research will suffer if biotechnology companies are unable to count on the collaboration of academic scientists and hospitals. In addition to these general concerns, BIO would like to offer comments on specific research issues directly affected by the medical privacy regulation.

Regulation of Clinical Research. Research activities of biotechnology companies already are subject to the regulations of the Food and Drug Administration (FDA), the state laws that apply to every research site where we collect information about research participants, as well as the federal regulations that govern the IRBs responsible for reviewing each of the projects where data are collected from patients that are receiving care or participating in research at an academic institution.[3] Research protocols typically involve data collected from individuals recruited by investigators affiliated with multiple separate institutions. As a result of the Common Rule, therefore, even without the new HIPAA requirements, the research protocols that companies sponsor, including the arrangements for safeguarding the privacy of participants and protecting the confidentiality of the data that is collected, are independently reviewed by IRBs at each institution where data are collected.

Nevertheless, to the already duplicative regime in existence under the Common Rule, the regulation adds new requirements. Specifically, it mandates a new privacy authorization form that addresses separate legal issues from the informed consent form under which each research participant agrees to participate in research and acknowledges the potential risks. For example, the form addresses whether the research participant agrees that information from the treatment that is part of the research protocol can be made available to the researcher. No deviations are allowed from any of the elements that are required to be in this new form unless the IRB specifically "waives" the form of authorization using a complex and subjective set of criteria. Nothing about this process is related to the privacy of individuals' information transmitted in connection with the transactions specified in the HIPAA statute. This new research review requirement is simply a modification of the Common Rule to add privacy as a separate risk factor with its own IRB review, separate from the IRB's consideration of other risks to research participants. The desirability of such a proposal must be addressed in the context of a broader consideration of the current federal research regulations, not added to the duties of academic medical centers and other covered entities involved in research as part of HIPAA.

De-Identified Information. Much useful research can be structured to protect privacy by creating incentives to use databases of de-identified information—information that does not identify an individual. Notwithstanding the Secretary's acknowledgement of this fact, the "safe harbor" criteria in the regulation for creating a de-identified database seem to be calculated to create data that are useless for research purposes. As a result, the regulation seems likely to have the incongruous result of encouraging researchers to seek review by an IRB, or to set up what the regulation calls a "privacy board" so that they can obtain data that are appropriate for research. BIO believes that de-identification appropriate to the researcher's proposed and permitted use of the data can be an effective means of protecting the confidentiality of data subjects. The regulation's use of a one-size-fits-all set of standards will deter people from taking these measures seriously in the research context.

Post-Marketing Surveillance. BIO also is concerned that the regulation misunderstands the FDA regulatory scheme under which doctors and hospitals voluntarily report information about product outcomes to companies that are responsible for collecting information and reporting to FDA any "adverse events." Companies collect information about unexpected events—often from health care providers—to detect which actually may be "adverse" events associated with use of a particular drug. By defining the permissible disclosure so strictly, and imposing serious penalties for infractions, the regulation may cause providers to be very conservative in selecting the few incidents to report.

The regulation permits reporting only of "adverse events" *and* such reports must be made to the entity "required to report" them. As such, the provider must make subjective determinations about whether events are "adverse". The provider also must look beyond the name of the manufacturer on the label to ensure that the manufacturer is the entity "required or directed" by FDA to collect and report adverse events. It would be a terrible unintended consequence if, in the name of complying with federal privacy laws, providers were hesitant to report unusual outcomes to the manufacturer whose "800" number is on the product label, because of an uncertainty about whether or not the event is truly "adverse" or the labeled manufacturer is the entity required to collect and report events.

---

[3] These federal research regulations are known as the "Common Rule" because they have been adopted and codified by 16 federal agencies that are involved in conducting or supporting research with human research participants.

The same problem arises in connection with exposure registries that are used to more systematically collect information on use of products by special sub-populations in order to identify any issues that may not have been detectable in the clinical trials that supported product approval. In some cases, FDA has authority to require or direct the manufacturer to operate these registries (e.g., fast-track approvals). In other cases, the manufacturer may be willing to conduct a registry and FDA may support the idea, but FDA does not have authority to "require or direct" the manufacturer to do so. The privacy regulation says that covered entities may participate in the registries that FDA has "required or directed" but not in those that manufacturers voluntarily operate—even if they operate them consistent with the FDA's guidance documents regarding registries. We see no indication in Congress' enactment of the HIPAA administrative simplification requirements—including its provision for the Secretary to issue regulations protecting the privacy of medical information—that Congress wished the Secretary to use HIPAA's civil and criminal penalties in a manner that would cause providers to be leery of participating in our nation's system for monitoring the safety and efficacy of prescription pharmaceuticals.

BIO urges a delay in the effective date of the regulations. A two year deadline for each of the separately issued elements of HIPAA has the potential to be harmful to research conducted with covered entities. Because requirements such as privacy and security are so closely related, most of the final arrangements for compliance with privacy cannot be addressed until the other is finalized.

BIO also supports changes that would help facilitate critical medical research. We are living in an era of enormous promise and potential clinical breakthroughs as scientists use genetic knowledge to improve our medical interventions. Decades of responsible science under the Common Rule has shown that protecting the confidentiality of data and promoting medical research are mutually attainable goals. Perhaps the time has come to reexamine the Common Rule to ensure that it still provides the kind of comprehensive protection for research participants that is integral to the conduct of high quality research. There have been many changes in our research infrastructure and our science since the Common Rule was adopted. BIO looks forward to working with the Committee as it pursues that goal.

Thank you.

Mr. BILIRAKIS. Has the gentleman completed his opening statement?

Mr. GANSKE. I yield back.

Mr. BILIRAKIS. Thank you. Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman. Let me mention part of my statement. I am disappointed that we did not hear from HHS or HCFA here today, because I believe there has been a great deal of misinformation spread about the final regulation put forth by the Clinton Administration. But I don't think anyone can argue with the fact that we do need uniform effective Federal guidelines in protecting an individual's right to privacy. People should not yield the right to privacy simply because they go to a doctor, contract an illness, take a diagnostic test, or suffer from a chronic disease.

Consensus does exist on the need for fair information practices from the health record. The bottom line is that medical records belong to the patient and should not be disclosed without their consent.

I look forward to this meeting and I hope we do get people from HCFA and HHS here to explain their implementations of the rule. I note that the subject matter of the hearing today is how to improve the medical record privacy regulations. If they are really not implemented yet, maybe we have the cart before the horse here, so I wish we had HCFA and HHS here.

So with that, I yield back my time, Mr. Chairman.

Mr. BILIRAKIS. I thank the gentleman.

Mr. Pitts for an opening statement.

Mr. PITTS. Thank you, Mr. Chairman. Thank you for holding this important hearing today on Federal medical record privacy. The recent growth in medical and computer technology and the continuing changes in technology have made health information an essential tool in our country's health care system. When I was young, our family went to our family doctor for nearly all of our medical care. Today, patients see a variety of health care practitioners, including specialists and alternative care providers. In this new environment, practitioners must be able to share and communicate about a patient's medical information. Accurate available health information is extremely vital to determining the best treatment for a patient.

Health information also is critical for basic insurance payments. Public and private payers need personal identifiable patient information primarily to pay billions of health care claims each year.

I recognize concerns with the confidentiality of their health information and agree that these concerns must be addressed, and that is why I do believe that we have need to have some standards protecting patients' medical records. However, as we work to protect individuals' identifiable health information, we must also make sure it is available for basic insurance and health plan functions.

Mr. Chairman, while I believe Congress has the responsibility to address consumer concerns, I also believe we must be careful not to adopt legislation that could undermine the health care industry's ability to provide these consumers with high-quality and affordable health care.

Again, I look forward to hearing from our distinguished panel of witnesses their thoughts today on the current medical privacy regulation and how we can improve it.

Thank you, Mr. Chairman.

Mr. BILIRAKIS. The gentleman from Wisconsin, Mr. Barrett.

Mr. BARRETT. Thank you very much, Mr. Chairman, and thank you for holding this hearing on this exceedingly difficult issue. I believe that the Clinton administration made a good-faith effort to address this issue after Congress failed to perform the duty it assigned itself. And I think that we have to be cognizant of that, that we were given the first kick at the cat and decided we would rather stand back and let somebody else do it.

So I have to give them credit for moving forward on the issue. At the same time, I think some opponents and critics of the rule have raised some serious questions which we must consider in the context of these rules. But the overriding concern that I have is that the privacy issue is real and the privacy issue is not going away. So we can run but we cannot hide when it comes to this issue. At some point we have to failings up to it. And I am glad that we have so many people here today to tell us their perspective on it and it is frankly much easier for me to learn when I am listening than when I am talking so I would yield back the balance of the time.

Mr. BILIRAKIS. The Chair thanks the gentleman for that. Mr. Greenwood for an opening statements.

Mr. GREENWOOD. Thank you, Mr. Chairman, for holding this hearing, and I thank the witnesses for appearing today. I appreciate this committee's resolve in addressing this important con-

sumer protection issue. Today I will introduce legislation to secure the confidentiality of patients' medical information. I do so because the final regulations promulgated by the Clinton administration currently under review by the Bush administration are in my opinion woefully inadequate. In fact, I consider them an abject failure. The final rule does not preempt State law. It imposes a silly construct for patient authorization for the use and disclosure of information that has little to do with privacy. It increases dramatically paperwork requirements on already burdened providers. The rule may increase medical errors and, therefore, unnecessary injury and death. It will likely inhibit medical research that benefits all Americans and it runs counter to Congress's efforts to double the budget of the NIH to improve clinical research, to expand patient access to clinical trials, to speed delivery of safe drugs, devices and biologics to consumers, and to bring Medicare into the 21st centry by covering prescription drugs.

Each witness here today will testify that the regulations are either unacceptable because they are onerous, or need to be expanded because they are inadequate. Quite frankly, that is not good enough. The final rule Secretary Shalala issued on December 28 fails health consumers and it fails America. It should be rejected, and comprehensive legislation should be enacted in its stead.

Janlori Goldman from Georgetown University will testify today that the final rule is a good starting point. She will say that all we need to do as a deliberative body is to build on the regulation's primal construct and we will seal the job of protecting medical health. I respect Ms. Goldman. I have worked closely with her, but I respectfully disagree with her on this point. The fact is, the final regulation embraces a dying concept in our society, one that embraces with bleary eyes a vision of the past that says we need only to lock medical files in crypts and file cabinets to ensure that our most intimate secrets remain undisclosed.

It is a dismal vision that fails to capitalize on new information technology that, while frightening to some, has the potential to protect our personal data better than any lockbox and skeleton key ever could. The regulation embraces a concept that artificial geographic boundaries are relevant in the Internet world and a global economy. It states that accidents of geography should determine relative data security. This vision ignores advances in research protections and encryption technology as no more relevant today than buggy whips and butter churns. It embraces an uneven patchwork quilt of differing standards that will leave consumers and providers confused, pondering the question of why we can't capitalize on newfound wonders of computer security, enhanced accountability, and secured trust. It will harm, not help consumers.

Finally, the regulation ignores the concept of the commerce clause embodied in our Constitution. For these reasons, we should lift our eyes from what we sought to secure in the past to what we might achieve in the future. We ought to reject this privacy rule and seek to bridge differences between Republicans and Democrats, liberals and conservatives, in order to find common ground that truly secures our most intimate secrets while advancing medical science. This rule seeks to lock in place where we have been, not

where we need to go. Other than that I think they are fine, Mr. Chairman.

Mr. BILIRAKIS. The gentleman's time has expired.

Mr. Green for an opening statement.

Mr. GREEN. Thank you, Mr. Chairman. I appreciate Mr. Greenwood's support for those regulations. Mr. Chairman, I will not give my total opening statement because I would like to hear from our panel, but obviously I disagree with my colleague. I think medical privacy is a very import issue and one that requires input from many different parties. I am pleased to see such a diverse group of witnesses today. I do wish a member from HHS was here, and hopefully before the Easter district work period we will be able to have someone.

Keeping personal information medical private has been the cornerstone of the medical profession since the dawn of time. When taking the Hippocratic oath, the doctor promises, "Whatever in connection with my professional service I see or hear . . . I will not divulge as reckoning that all such shall be kept secret."

Unfortunately, medical information is no longer stored in filing cabinets in an office. Advances in technology mean that these records are on computers and they can be transferred very easily and accessed with a few keystrokes. We have heard the horror stories. What worries me is that 1 in 6 patients withhold information from their doctors because they fear it will not be protected. Without adequate information, doctors are hobbled in their ability to diagnose and treat patients, and the result is the patients risk an undetected and untreated condition which could escalate to even more painful and costly illnesses.

There is a need for medical privacy regulations. I share my colleague from Pennsylvania's concern, and hopefully we can work together. I know there are groups on both sides of the aisle who want to see some changes, but I would hope this administration would not take civil steps to kill this medical privacy regulation. We saw what happened with the ergonomics rule that we took 10 years to create. We see what is happening with a number of regulations on environment. This is not setting a pattern for the bipartisan efforts that President Bush talked about. But I would hope that if we do need to make some changes in the regulations, that we can work together.

And I yield back my time.

Mr. BILIRAKIS. The Chair thanks the gentleman.

Mr. Bryant.

Mr. BRYANT. Thank you, Mr. Chairman. I apologize for shuffling back and forth, but I am trying in the same day—I am trying to learn about medical privacy as much as possible, and electricity in California upstairs. And I also thank you for having this hearing and my consideration of wanting to hear from this panel.

I will yield back my time, but probably the main reason I came back was to hear Mr. Markey's statement.

Mr. BILIRAKIS. Yes. Mr. Markey has been patiently waiting. Mr. Markey is not a member of the subcommittee, but has requested to make a very short opening statement. Without objection, he will now be recognized.

Mr. MARKEY. Thank you, Mr. Chairman. Thank you for your courtesy. Obviously the reason why so many members and so many Americans are now concerned is that over the last couple of weeks there have been a startling number of decisions that have been made by the Bush administration which have given us cause to be concerned about what could now happen to these privacy regulations. The gentleman from Texas, Mr. Green, alluded to the worker safety rules. Obviously there was a decision made on CO2, whether or not it is a pollutant, which helps to dramatically increase the problem of greenhouse gases causing global warming problems. And then there is the arsenic decision that was just made, you know. And obviously if they can make a decision on arsenic, then they can definitely make a decision on privacy that hurts public health and safety.

Until this week EPA stood for the Environmental Protection Agency. Now it stands for "Eat Plenty of Arsenic." There is absolutely no rationale for making that kind of a change. There is a Dickensian quality to the wires that have been installed over the last 10 years in this country: It is the best of wires and it is the worst of wires, simultaneously. It can enable and ennoble or it can degrade or debase simultaneously. We just cannot pretend that it is all good. It is not.

All that information in your financial records, in your health records, in everything else you do, can now be compiled into a digital dossier that allows some company to know more about you than you know about yourself. But, moreover, when it comes to your health care records, it makes it possible for them to basically spread information that only you want to know. You might not have told anyone else in your family, much less everyone else in town, every company that is out there. So you should have a right to be able to protect yourself. I think that basically is the core right that we should all have. If there is a bottom-line core privacy right that we have should have, it is to our own medical information, our own DNA, who we are. We should be able to control that.

And whether or not you are on ESPN.Com or bought a book at Amazon.com, we can debate over that; but over who we are, who our family members are, husbands, wives, children, mothers, fathers, you know, we should have a right to know that it is going to be protected.

So you have these information reapers now who are out there trying to gather this profile that they will be able to make money off of, replacing the information-keepers that we grew up with, that nurse, that doctor in the hometown, who we knew was never going to tell anyone about it. But the privacy peepers now do not just kind of learn a little secret about you, they also make money off of it. That is the fear: The more they learn about you is the more money they make. And that is why America is afraid, because they might ultimately decide in large numbers not to get the health care treatment which they need.

And that is why privacy is going to be the civil rights issue of the next generations. Because this wire, this new digital built stream, makes it possible for all of this information to be gathered about people.

Now, on April 15, we have tax day. On April 14, HHS has to make a decision as to whether or not they are going to protect America's privacy. Now, I say "No Taxation Without Implementation" of the health care privacy regulations. I think it would be a tragedy if people in the same week lost their privacy and had to pay their taxes. And in the long run, the loss of privacy would be a much greater harm for these families to suffer when it came to all of the medical secrets that they have.

So, Mr. Chairman, I don't think we are going to have a more important hearing this year, and I hope that HHS does the right thing for the American people on this subject.

I yield back the balance of my time.

Mr. BILIRAKIS. I thank the gentleman. I note that we are happy that he did not insist as to privacy on his opening statement. But he has been a strong supporter of privacy throughout the years. I know we have heard an awful lot from Mr. Markey on this subject as well.

Mr. MARKEY. Mr. Chairman, I have a letter from 50 Members to the Secretary of HHS on the subject. Could I insert it in the record?

Mr. BILIRAKIS. I suppose there is no problem with your inserting that into the record. That will be the case.

[The letter referred to follows:]

CONGRESS OF THE UNITED STATES
WASHINGTON, DC 20515
March 20, 2001

The Honorable TOMMY THOMPSON
Secretary of Health and Human Services
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

DEAR SECRETARY THOMPSON: We are writing to express our concern with the recent decision to open a new 30-day comment period on the final medical information privacy standards mandated by the Health Insurance Portability and Accountability Act (HIPAA). The health privacy of Americans has been on hold for far too long, and we respectfully urge you to put these important privacy protections into effect night away.

This long-overdue regulation establishes for the first time a fundamental right to medical privacy. This new standard includes access to one's own medical records, a requirement of notice of how health information is going to be used and shared, a requirement of consent for use and disclosure, and limitations on employer access to personal health information.

At this point, further delay of these crucial protections would be a major setback in years of effort to grant Americans the privacy they have demanded for so long. Americans have waited long enough for privacy protections, and every day that this rule is not in effect, the confidentiality of their patient records are at risk. Therefore, we urge you not to delay these protections any further.

The process of developing the current regulation has been open and extensive. HIPAA, which passed with strong bipartisan support in both Houses in 1996, included a three-year deadline for Congress to pass a comprehensive medical privacy law. Understanding the importance of this issue, Congress built in a back-up plan giving the Secretary of Health and Human Services (HHS) the authority to promulgate a health privacy regulation in the absence of legislation by August 1999.

Over the years that this regulation was developed, the views of Congress and interested parties were given ample consideration. In September 1997, the Secretary of HHS presented recommendations to Congress for legislation on medical privacy. Subsequently, several bills were introduced but no law was passed. HHS then issued a proposed rule in November 1999, and even extended the comment period by 45 days at the request of industry and consumer groups. The Department then considered more than 52,000 comment letters over ten months before issuing a final rule.

We recognize that special circumstances may arise from time to time that are not fully anticipated in the regulation. For this reason, HHS is authorized in section 262 of HIPAA to work with the healthcare industry, providers, and consumers to resolve potential problems with compliance on a case-by-case basis. However, this process cannot begin until the covered entities move forward with implementing the rule.

We strongly urge you to hold the line on medical privacy by allowing the regulation to take effect on April 14th as originally provided. Americans have waited too long for these critical privacy protections—they shouldn't have to wait any longer.

Sincerely,

EDWARD J. MARKEY, *Member of Congress;* EDWARD M. KENNEDY, *United States Senate;* HENRY WAXMAN, *Member of Congress;* PATRICK LEAHY, *United States Senate;* JOHN D. DINGELL, *Member of Congress;* CHRISTOPHER J. DODD, *United States Senate;* RICHARD A. GEPHARDT, *Member of Congress;* THOMAS A. DASCHEL, *United States Senate;* GARY A. CONDIT, *Member of Congress;* TOM HARKIN, *United States Senate;* EDOLPHUS TOWNS, *Member of Congress;* JEFF BINGAMAN, *United States Senate;* BILL LUTHER, *Member of Congress;* JACK REED, *United States Senate;* ROSA L. DELAURO, *Member of Congress;* HILLARY RODHAM CLINTON, *United States Senate;* PETE FORTNEY STARK, *Member of Congress;* JOHN F. KERRY, *United States Senate;* JIM MCDERMOTT, *Member of Congress;* JOHN D. ROCKEFELLER, *United States Senate;* JAMES P. MORAN, *Member of Congress;* ROBERT G. TORRICELLI, *United States Senate;* JANICE D. SCHAKOWSKY, *Member of Congress;* DANIEL K. INOUYE, *United States Senate;* GEORGE MILLER, *Member of Congress;* DANIEL A. AKAKA, *United States Senate;* JOHN P. MURTHA, *Member of Congress;* JON CORZINE, *United States Senate;* DENNIS KUCINICH, *Member of Congress;* PATSY MINK, *Member of Congress;* MAURICE HINCHEY, *Member of Congress;* DALE E. KILDEE, *Member of Congress;* JOHN F. TIERNEY, *Member of Congress;* JAMES P. MCGOVERN, *Member of Congress;* ANNA ESHOO, *Member of Congress;* LUCILLE ROYBAL-ALLARD, *Member of Congress;* SHELLEY BERKLEY, *Member of Congress;* JERROLD NADLER, *Member of Congress;* JOSÉ SERRANO, *Member of Congress;* CAROLYN B. MALONEY, *Member of Congress;* ELEANOR HOLMES NORTON, *Member of Congress;* JIM TURNER, *Member of Congress;* WM. LACY CLAY, *Member of Congress;* BOB FILNER, *Member of Congress;* ROBERT A. BORSKI, *Member of Congress;* SHERROD BROWN, *Member of Congress;* PAUL WELLSTONE, *United States Senate;* JULIA CARSON, *Member of Congress;* and JOHN EDWARDS, *United States Senate.*

Mr. BILIRAKIS. All right. We are going to break now. I will ask all of the witnesses to please take their seat so that as soon as we cast this vote and return, we can continue on.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Let me begin by thanking Subcommittee Chairman Bilirakis for holding this timely hearing on the Federal medical record privacy regulation, which is now the subject of a comment period that expires at the end of the month.

The Energy and Commerce Committee has already held two hearings this year on privacy. This hearing, of course, will focus on medical privacy, an area of the law that raises a host of important issues for consumers and health care providers.

The specific purpose of this hearing today will be to examine a regulation that was issued in the closing days of the Clinton Administration. Once the new Administration has time to review the comments they are receiving on this regulation, we will bring Secretary Thompson's team forward and hear their thoughts about how the regulation can be improved. As I told my good friend Mr. Dingell this week, we are working to arrange a time to host Secretary Thompson or his designee at a hearing before this Committee so that we can inquire further into their positions on this privacy regulation.

We all want to be sure that our medical records are kept private, and this is not a new concern. In fact, the Hippocratic Oath states that "Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." Physicians have subscribed to these tenets since at least the 4th Century B.C., and these principles still apply today.

Unfortunately, in the interconnected 21st Century, relying on the Hippocratic Oath isn't good enough. Records are reduced to electronic form and shipped from one part of the country to another for diagnosis, payment, fulfilling prescriptions, or epidemiological research. Every American wants to know that their medical records remain confidential, and that sensitive medical information identifiable to

them, is not bought, sold and displayed on the Internet. No one deserves to have that happen to them. We want to be assured that personally-identifiable health information is protected from public disclosure, and that privacy safeguards are developed that would complement rather than burden biomedical research. Moreover, we need to make sure that workable security systems are in place safeguarding the privacy of the medical records of American citizens. All of the protections on the books won't help consumers unless we can prevent criminals from breaking into computers and improperly accessing patients' medical records.

And that's why we are here today—to discuss these issues. During this hearing, we want to examine the implications of moving forward with the Clinton Administration's privacy policy. While we have no doubt that drafting this regulation was an arduous process, and an unenviable task, we still need to explore how we can improve this regulation and make it work more effectively for consumers and health care providers.

We all want today's hearing to be constructive. For example, I hope that we can hear about what parts of the regulation could be strengthened from a consumer's point of view. How can we better draft this regulation to bring these new protections to consumers in a more cost-effective way? What provisions need a little more fine-tuning in light of real-life practices? These are the kinds of issues we would like to explore today.

Mr. Chairman, thank you again for holding this hearing. I look forward to hearing the testimony and learning more about these issues.

PREPARED STATEMENT OF HON. EDOLPHUS TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

I am hopeful that today's hearing rather than delaying medical privacy rules actually will move us one step closer to the implementation of the final rule on April 14th.

As a former hospital administrator, I can speak from personal experience about how the climate has changed for the privacy of medical records. Doctors no longer simply maintain patient records under lock and key in a file cabinet. Today health information is both in paper and electronic form leaving patient privacy and confidentiality largely unprotected.

Nowhere are these protections of more concern than in the area of on-line privacy of medical records. New initiatives like informatics—the science of optimizing the storage, retrieval, and management of information found in patient records and medical databases—will revolutionize the traditional doctor-patient relationship. Experts argue that on-line medical records can improve the quality of healthcare through better efficiency, lower costs and the elimination of thousands of medical errors. I don't doubt that these improvements would occur. Confidentiality, however, can be a significant weakness in these systems.

For example, there is nothing to prohibit a hospital employee from "snooping" through a patient's record. In fact, yesterday's Supreme Court case, decided in favor of patient protection, arose from the overzealous decision by a hospital staff member to share positive drug test results from pregnant women with local law enforcement in Charleston, South Carolina. In fact, in many instances, an on-line review by an employee would be assumed to be authorized as part of that patient's care.

Consequently, given the patchwork nature or in some cases the total absence of a privacy standard, April 14th becomes absolutely critical in terms of establishing a national standard for the protection of medical records. As the Ranking Member on the Subcommittee on Commerce, Trade and Consumer Protection, I anticipate that we will continue to examine e-commerce and privacy issues. It is my expectation that the national standard established by this medical privacy rule will guide our future considerations in the on-line privacy debate. This linkage makes it even more important for the rule to be finalized.

Americans have waited long enough for medical privacy protections. I would urge Secretary Thompson to allow this rule to go into effect to create a privacy system that covers all health information held by hospitals, providers, health plans and health insurers. I am hopeful that our witness testimony today will support the finalization of this rule.

PREPARED STATEMENT OF HON. ANNA ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

The American people expect, and are entitled to, confidential, fair and respectful treatment of their private health information. Currently, we do not have a federal

standard, and the existing patchwork of state laws provides erratic protection at best.

With the advent of managed care, patients can no longer depend on their family doctor to protect their confidentiality. Instead they are forced to place their trust in entire networks of insurers and health care providers with direct access to their sensitive medical information.

The need for meaningful privacy protections is clear. Yet President Bush has arbitrarily decided to delay implementation of HHS regulations that would have provided them. The stated reason for the delay was to enlist further public comment, yet HHS has already received 53,000 comments prior to issuing the final rule. I'm dismayed by the President's seeming callous disregard of our constituents' call for privacy protection and I hope that the purpose of this hearing is to help move the issue along rather than an effort to help stall implementation.

As this Committee moves toward a solution to the privacy dilemma, I urge my colleagues to keep in mind the need to balance meaningful privacy protection with our interest in medical research. When we held hearings on this issue last year, I cautioned my colleagues that any legislation or regulation enacted should not erect unnecessary barriers to the ability to conduct medical research.

I'm encouraged that my concerns appear to have been heard and the regulations include flexibility in the IRB structure applied to privately funded research. For example, the regulation allows expedited review for research on archived medical records. This is significant since information is the lifeblood of research. Without access to health data, patients would be the real losers.

Mr. Chairman, our constituents have demanded that their federal representatives provide them with a meaningful federal standard to protect against unauthorized uses of their most private health information.

At the same time, we must also ensure that these protections incorporate the appropriate flexibility to continue needed medical research. I believe the regulations put forth by the Clinton Administration go a long way toward achieving these two goals.

Thank you Mr. Chairman. I look forward to hearing from the witnesses.

[Brief recess.]

Mr. BILIRAKIS. Let's have order, please. For the benefit of those who ordinarily do not come up here to testify, this is a very rude thing to do to you, and certainly very discourteous. We can't help it. When votes are called, we have to run over, and we hope you realize that. We understand that in just a few minutes we have a series of votes coming up, so there will be another series of votes before we have to break again.

The Chair welcomes and thanks the witnesses, consisting of Dr. John D. Clough, Director of Health Affairs for the Cleveland Clinic Foundation; Ms. Mary Foley, President of the American Nurses Association; Dr. John Melski, Medical Director of Informatics at the Marshfield Clinic in Marshfield, Wisconsin; Dr. Paul Appelbaum, Chairman of the Department of Psychiatry, University of Massachusetts Medical School; Mr. Carlos R. Ortiz, Director of Government Affairs, CVS Pharmacy; Ms. Janlori Goldman, Director of Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University; and Mr. Bob Heird, Senior Vice President, Anthem BlueCross BlueShield. Welcome.

Your written statement is a part of the record. We would hope you would complement it orally. The clock is set for 5 minutes. Obviously, if you are not completely finished, we will let you go on, but at the same time keep it as close to that as you can.

We will start off with Dr. Clough. Is that the correct pronunciation?

Mr. CLOUGH. Correct.

Mr. BILIRAKIS. There has been a Dr. Clough in Tarpon Springs, Florida for many, many years.

Mr. CLOUGH. Probably a distant relative.

STATEMENTS OF JOHN D. CLOUGH, DIRECTOR OF HEALTH AFFAIRS, CLEVELAND CLINIC FOUNDATION; MARY E. FOLEY, PRESIDENT, AMERICAN NURSES ASSOCIATION; JOHN MELSKI, MEDICAL DIRECTOR OF INFORMATICS, MARSHFIELD CLINIC; PAUL APPELBAUM, CHAIRMAN, DEPARTMENT OF PSYCHIATRY, UNIVERSITY OF MASSACHUSETTS MEDICAL SCHOOL; AND CARLOS R. ORTIZ, DIRECTOR OF GOVERNMENT AFFAIRS, CVS PHARMACY

Mr. CLOUGH. Good morning, Chairman Bilirakis, Vice Chairman Norwood, Mr. Brown, and distinguished members of the committee. I am Dr. John Clough, director of health affairs at the Cleveland Clinic. I have also been a practicing rheumatologist for 30 years. I thank you for allowing me——

Mr. BILIRAKIS. Your mike, sir. Please pull it closer. We do want to hear what you have to say.

Mr. CLOUGH. I thank you for allowing me to offer testimony today on behalf of American Medical Group Association, the AMGA, and the Health Care Leadership Council, HLC.

The AMGA represents approximately 300 medical care groups which care for 35 million patients nationwide. The HLC represents CEOs of the Nation's leading health care companies and institutions, including hospitals, and the Cleveland Clinic is a member of both.

Medical group providers strongly support the confidentiality of patient information and appreciate the Department's efforts in this respect. The HLC and AMGA support creating workable, nationally uniform standards that protect confidentiality, including the rights of patients to inspect their records, notice of confidentiality practices, safeguards for information, and prohibition of unauthorized disclosure of patient information for purposes other than treatment, payment, health care operations and research.

The final HHS regulation contains several improvements from the originally proposed regulation. Nevertheless, I would like to highlight three key provisions that appear to be unworkable, would disrupt patient care, would divert limited resources from treating patients. These are the prior consent requirement, the minimum necessary standard, and the rules governing disclosure of information to business associates.We need to delay the implementation of the rule until these issues are appropriately addressed.

In terms of prior consent, in a major departure from the proposed rule, HHS created a prior consent mandate on providers. This unprecedented mandate would require doctors to obtain a signed written consent from patients before using or disclosing patient information for even the most routine purposes, including treatment. This is unworkable for several reasons. The task for physicians and the cost to medical groups to obtain such consents for more than 200 million Americans is daunting. No State of which I am aware currently requires prior consent to use or disclose information for treatment. This requirement will disturb a range of routine provider practices from sending out reminder notices about appointments, to conducting disease management and maintaining quality improvement programs. It could force patients to make an extra trip to the hospital to sign consent forms before a hospital can use any medical information about them.

Here is one of many examples of how the rule could disrupt routine patient care. Today, increasing numbers of surgical procedures are performed in the outpatient setting. Now, if I refer a patient for outpatient surgery, he or she would not have to go to the ambulatory surgery facility until the day of the operation. Under the new consent requirement, however, the patient would have to make a special trip to sign the necessary consent forms before the operation could even be scheduled. To add to the confusion, the patient must be given the opportunity to restrict or revoke the consent at any time. But what if the patient revokes consent for use of information supporting payment but the information is also needed for key health care operations such as infection tracking, quality assurance, outcomes assessment and so on?

The prior consent requirement dehumanizes the relationship between patient and physician, a relationship that is built upon patient trust that a physician will use good professional judgment to determine the use of the patient's information, particularly in care management.

We recommend that HHS eliminate this overly burdensome and costly requirement and return to the statutory authorization as in the originally proposed rule. In the case of "minimum necessary" in today's coordinated systems of health care delivery, information sharing and use by teams of physicians and other health professionals is the key to the quality, efficiency, and effectiveness of medical care and prevention, detection, and mitigation of medical errors. The minimally necessary provision is not necessary itself, especially as it applies to internal uses of patient information. The regulation should allow health care providers to develop their own set of guidelines and rules based on what is best for the patient.

Finally, as to business associates, rewriting contracts with every entity to which the Cleveland Clinic discloses patient information in order to achieve compliance with this regulation will require a substantial amount of legal and professional time, effort, and expense. We believe that these problems can be addressed and the rule can move forward, but rushing forward on a flawed and unworkable regulation could hinder the cause of protecting and improving the quality of health care. It makes sense to get the regulation right the first time, before hospitals and others have spent limited resources to comply with the rule that has to be changed.

Therefore, we urge the Department to delay the April 14, 2001 effective date to give the Department adequate time to consider the many comments it will receive. Once these comments are carefully considered, a new version of the rule fixing the problems we have identified can be promulgated with our support.

Thank you very much.

[The prepared statement of John D. Clough follows:]

PREPARED STATEMENT OF JOHN D. CLOUGH, DIRECTOR, HEALTH AFFAIRS, CLEVELAND CLINIC FOUNDATION ON BEHALF OF THE AMERICAN MEDICAL GROUP ASSOCIATION AND THE HEALTHCARE LEADERSHIP COUNCIL

Good morning, Chairman Bilirakis and members of the subcommittee.

I am Dr. John D. Clough, Director of Health Affairs, Cleveland Clinic Foundation. I am also a practicing rheumatologist. I offer testimony today on behalf of the American Medical Group Association (AMGA) and the Healthcare Leadership Council (HLC).

The AMGA represents approximately 300 medical groups that care for 35 million patients nationwide. The HLC represents the CEOs of the nation's leading health care companies and institutions.

Thank you for giving me this opportunity to testify on the HHS regulation. Medical group providers strongly support the confidentiality of patient information. We appreciate the Department's effort to create meaningful and balanced federal standards to protect the security of each individual's health information.

The HLC and AMGA support creating nationally uniform standards protecting confidentiality, including giving patients the right to inspect their records, notice of confidentiality practices, creating safeguards for information, and prohibiting disclosure without authorization of patient information for purposes other than treatment, payment, health care operations, and research.

The final HHS regulation contains several improvements from the proposed regulation. However, I would like to highlight three key provisions that are unworkable, would disrupt patient care, and divert limited resources from treating patients: The prior consent requirement, "minimum necessary" standard, and "business associates."

Prior Consent

In a major departure from the proposed rule, HHS created a prior consent mandate on providers. This unprecedented mandate would require doctors to obtain a signed, written consent from patients before using or disclosing patient information for even the most routine purposes, including treatment. This mandate is unworkable because:

- The task for physicians and the cost to medical groups of obtaining such consents from over 200 million Americans is daunting.
- In no state of which we are aware do doctors routinely obtain prior consent to use patient information for treatment.
- As of the compliance date for the HHS regulation, no physician will be able to use information for most activities without a signed consent. Thus, routine practices by providers will be disrupted, from sending out reminder notices about appointments to conducting disease management and maintaining quality assurance programs.
- This requirement could force patients to make an extra trip to the hospital to sign a consent form before the hospital can use any medical information about them.
- More and more surgeries are on an outpatient basis today. Currently, if I see a patient and refer her to have an outpatient surgical procedure, she would not have to go to the outpatient facility until the day of the surgery. With the new consent requirement, however, she would have to make a special trip to sign the necessary consent forms before the outpatient facility could use her information to schedule surgery and initiate the intake process.
- To add to the confusion, a patient must be given the opportunity to restrict or revoke the consent at any time. This poses significant difficulties for group practices. What if there is a restriction on, or revocation of, a consent for payment or health care operations and the information is needed for billing or key health care operations such as infection tracking, quality assurance, outcome assessments, and so on?

The prior consent requirement de-humanizes the relationship between the patient and physician—a relationship that is built upon patient trust that a physician will use good professional judgment to determine the use and disclosure of the patient's information, particularly in the course of treatment of the patient. We advocate that HHS should eliminate such an overly burdensome and costly requirement and return to the statutory authorization as under the proposed rule.

Minimum Necessary

Most health care services today are delivered in some form of organized or coordinated system of delivery. Information sharing and use by teams of physicians and health professionals is the key to quality medical care for patients, and the key to improvements in patient care. The sharing of information among health care professionals in an integrated system is critical to their ability to serve patients in the most efficient and effective way.

Under the rule, providers must make reasonable efforts to limit the use and disclosure of information to what is minimally necessary to accomplish its intended purpose. Under the final rule, disclosures and requests are excluded from the requirement; however, there is no such exclusion for "use" of information. This potentially limits the ability of providers to use a complete medical record for treatment purposes. The concept of limiting the use of the full medical record for treatment

purposes would appear to be completely contrary to efforts to prevent medical errors and promote patient safety.

This provision is unnecessary, particularly to the extent it applies to internal uses of patient information. Rather than establish a minimum necessary standard, the regulation should allow health care providers to develop their own set of guidelines and rules about what they believe is the necessary standard and what is best for the patient.

Business Associates

Rewriting and recontracting with every entity to whom Cleveland Clinic discloses patient information in order to achieve compliance with this regulation will require a substantial amount of legal and professional time, effort and expense. Last week, Secretary Thompson testified regarding the need to ensure administrative simplification of complex and burdensome regulations. Also, the underlying intent of the section of HIPAA in which privacy falls is "administrative simplification."

Yet, the "business associate" requirements would necessitate hundreds, and for some entities, thousands of privacy contracts. We recommend that the business associate provision be removed because HHS has exceeded its statutory authority under HIPAA. We especially object to a requirement of a contract between covered entities and business associates.

We believe that these problems can be addressed and the rule can then move ahead. Rushing forward on a flawed regulation that is unworkable could set back the cause of protecting confidentiality and improving the quality of health care. It makes sense to get the regulation right the first time, before hospitals and others have spent limited resources on complying with a rule only to see it changed. Therefore, we urge the Department to delay the April 14, 2001, effective date to give the Department adequate time to consider the many comments it will receive. Once these comments are carefully considered, a new version of the rule fixing the problems we have identified can be promulgated with our support.

Mr. BILIRAKIS. I thank you. Ms. Foley.

STATEMENT OF MARY E. FOLEY

Ms. FOLEY. Thank you, Mr. Chairman, and members of the subcommittee. I am Mary Foley, registered nurse and president of the American Nurses Association, which is the only full service professional organization that represents our Nation's registered nurses in all 53 State and territorial nursing associations.

It is a great pleasure to be here this morning and offer our views on patients' privacy and confidentiality regulations as issued by the Department of Health and Human Services in December of last year. Mr. Chairman, as I indicated, I am a health care practitioner, and until I came president of the American Nurses Association just over a year ago, I was a nurse executive in a medium-sized hospital in urban California. Before that I spent 17 years as a staff nurse at that hospital, and I have also been a clinical instructor in nursing.

The second charge in the code for nurses, our ethical code, states, "the nurse safeguards the client's right to privacy by judiciously protecting information of a confidential nature." That very simple statement is an obligation that our profession takes very seriously. Virtually all of our members are involved in creating, transmitting, maintaining, and safeguarding patient records on a daily basis as an integral part of their professional practice. Working on the front line of health care, registered nurses are well aware of the concerns their patients have regarding privacy and confidentiality. We remain professionally committed to strong, enforceable standards to protect the confidentiality of the health information of our patients. This commitment has always been a part of the professional practice.

In my testimony this morning I will focus on two aspects of this issue that I can speak to as a nurse and as a representative of the nursing profession. First, it is the necessity to keep our focus on what is best for patients; and, second, it is the practical application of this standard in health care settings. The most important test that these regulations must meet is whether every individual patient's reasonable expectation for privacy and confidentiality is addressed. Can I assure my patients when they are describing the most intimate, troublesome, embarrassing, frightening aspects of their lives to people who will treat and care for them that there are safeguards for maintaining the confidentiality of this sensitive and important information? Mr. Chairman, if I can't do that, many of my patients and many around this country will go without treatment or will disclose only some of the information, a very dangerous proposition which can lead to improper diagnosis, improper treatment, complications in an illness or injury, negative drug interactions, adverse events, or even death.

It is hard to talk about a whole range of sensitive issues which might include mental illness, sexual practices, and physical abuse. It will not happen at all if you think your story is going to be grist for the local gossip mill or sold to a corporation that will farm it out to telemarketers in case you might be in the market for a pregnancy test, or also that it could be available to your employer who would then have the opportunity to consider the implications perhaps for your prescription for antidepressants.

This concern for our patients must be our overriding concern, not whether the rule will be inconvenient for hospitals or practitioners or for the staff people who handle insurance paperwork.

This regulation requires that a covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure. And, of course, it must. Our accrediting bodies for hospitals already require that. Any suggestion that this is new or burdensome for health care institutions is really unfounded. You watch your voice, you don't talk about patients by names in the hallways. You post prominent notices in their predominant languages for patients, informing them that the staff will work to meet their request for greater privacy, and then follow through on it. We were already complying with the intent.

These instructions are the stuff of daily work in a hospital setting and every nurse is trained to be in tune to its importance. And any hospital or practitioner that isn't already doing it, and doing it seriously, is a menace. Every day there are practitioners who, as a matter of ethics and successful treatment, must be able to ensure their patients that their records are protected. We have a patchwork of State laws that provide some protections to some people, some of the time, in some places. We need this national standard for basic protections for all of our people, all of time, in every place in this Nation.

Thank you Mr. Chairman. I remain available to answer any questions.

[The prepared statement of Mary E. Foley follows:]

PREPARED STATEMENT OF MARY E. FOLEY, PRESIDENT, AMERICAN NURSES ASSOCIATION

Mr. Chairman and Members of the Subcommittee: I am Mary Foley, President of the American Nurses Association, which is the only full-service professional organization representing the nation's registered nurses through our 53 state and territorial nurses associations. It is a pleasure to be here this afternoon to offer our views on the patient privacy and confidentiality regulations issued by the Department of Health and Human Services in December of last year.

Mr. Chairman, I am a health care practitioner. Until I became President of the American Nurses Association just over a year ago, I was a nurse executive in a medium-sized hospital in California. Before that, I spent seventeen years as a staff nurse, and I have served as clinical instructor in nursing.

The second charge in the Code for Nurses states, "The nurse safeguards the client's right to privacy by judiciously protecting information of a confidential nature." That simple statement is an obligation the nursing profession takes very seriously.

Virtually all of ANA's members are involved in creating, transmitting, maintaining, and safeguarding patient records on a daily basis as an integral part of their professional practice. Working on the front line of health care, registered nurses are well aware of the concerns of their patients regarding privacy and confidentiality and are professionally committed to strong enforceable standards to protect the confidentiality of the health information of their patients.

This commitment has always been a part of professional practice. But the need for Federal law is in large part a function of the momentous change in communications technology. Health care professionals have always been aware of the importance of confidentiality and the possibilities for carelessness; the need for that reminder in the code of ethics is real. But the complexity of the health care system means that transgressions of patient confidentiality, intentional or not, have much broader consequences than ever before, because the information travels further and faster and cannot be retrieved.

In my testimony, I will focus on two aspects of this issue that I can speak to as a nurse and as a representative of the nursing profession: First, is the necessity to keep our focus on what is best for the patient. Second, is the practical application of this standard in health care settings.

The most important test that these regulations must meet is whether every individual patient's reasonable expectations for privacy and confidentiality are addressed. Can I assure my patients that " when they are describing the most intimate, troublesome, embarrassing, frightening aspects of their lives to people who will treat them and care for them " there will be safeguards for maintaining the confidentiality of this sensitive information?

Mr. Chairman, if I can't do that, many of my patients will go without treatment or will disclose only some of the information, a dangerous proposition, which can lead to improper diagnosis, improper treatment, complications in an illness or injury, even death. It is hard to talk about a whole range of sensitive issues, which might include mental illness, sexual practices, and physical abuse. And it will not happen at all if you think your story is going to be grist for the local gossip mill or sold to a corporation that will farm it out to telemarketers in case you might be in the market for a pregnancy test or be available to your employer, who will have then the opportunity to consider the implications of a prescription for antidepressants.

This concern for our patients must be our overriding concern, not whether the rule will be inconvenient for hospitals or practitioners or staffers who handle insurance paper work.

This regulation requires that "a covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure . . ." Of course it must. Accrediting bodies for hospitals already require it. Any suggestion that this is a new or burdensome requirement for health care institutions is really unfounded. Watch your voice, don't talk about patients by name in the hallways, post prominent notices for patients informing them that staff will work to meet their requests for great privacy—and do it. These instructions are the stuff of daily work in a hospital setting. Every nurse is trained to be attuned to its importance. And any hospital or practitioner that isn't already doing it—and doing it seriously—is a menace.

The American Nurses Association has long been in the forefront of organizations that have worked for better and more standardized electronic communications among health care providers as an important improvement in patient treatment and care. It is clear that the work in this area undertaken as a result of the Health Insurance Portability and Accountability Act will provide a huge cost benefit to plans

and providers, as well. For the health care industry to accept this financial boon and then attempt, as is apparent in recent weeks, to weaken or impede these important safeguards to patient privacy and confidentiality is unfortunate and counterproductive.

We believe that this rule should go forward as issued. Congress ordered the Department of Health and Human Services to develop and promulgate this standard, absent Congressional action in the three years following enactment of the Health Insurance Portability and Accountability Act. The Department issued the standard as directed, after having sought and worked through an immense number of comments from a full range of stakeholders in the process. It is certainly remarkable to hear that some stakeholders believe that they have not been afforded a full opportunity to be heard. As would be expected, changes were made in the proposed rule in response to comments. The Department was careful to point out in its request for comments areas in which more information was wanted, such as the approach on requirements for patient consent. No final rule can ever be issued if it is always subject to additional comment. It is clear from a decade of Congressional attempts to fashion legislation on this issue that not all stakeholders will agree on some aspects of the issue, but the paramount concern must be the continuing and growing need for the regulation.

Are there issues that ANA considers important for future regulatory or legislative action? Yes. There is still inadequate protection for occupational health nurses who are daily pressured by their employers for access to information about employees who are treated at the work place. There is still no private right of action for individuals whose identifiable health information is recklessly disclosed. There is still inadequate protection from the use of private information for marketing purposes—the essence of privacy is the right to be left alone. There are still inadequate restraints on law enforcement access to information.

But these issues—and issues that may trouble other providers, consumers, or covered entities—may be dealt with in the future through legislation or regulation. Congress wisely in 1996 recognized that a legislative remedy could be difficult to achieve and wisely recognized that health privacy and confidentiality are far too important to be left subject to the vagaries of a difficult legislative environment.

We come back to our original point: for nurses, the first issue is protecting our patients. The regulation as issued is too important to be delayed or rescinded. There is time, if efforts are made in good faith, for covered entities to comply with this regulation. And there are administrative and—of course, ultimately—legislative remedies available for any aspect of the rule that should prove to be unworkable.

In the meantime, every day there are practitioners who, as a matter of ethics and successful treatment, must be able to assure their patients that their records are protected. We have a patchwork of state laws that provide some protections to some people some of the time in some places. We need this national standard of basic protections for all of our people all of the time in every place in the nation.

Mr. BILIRAKIS. Thank you very much, Ms. Foley.

Dr. Melski.

STATEMENT OF JOHN MELSKI

Mr. MELSKI. Thank you, Chairman Bilirakis, for the opportunity to speak to the House Subcommittee on Health, and special thanks to Representatives Sherrod Brown and Tom Barrett.

I speak to you as a physician whose code of ethics recognizes the solemn duty for confidentiality of what our patients reveal to us. And I also speak to you as Medical Director of Informatics, whose mission is to ensure that no patient ever suffer and to make sure that information is always available, whenever and wherever needed. Thus, my entire professional life is a struggle for a balance between concealment and revelation.

As technology has advanced and the demand for both concealment and revelation has increased, the stakes have become higher. I am here to bear witness that some of the well-intentioned provisions in the privacy regulations may have undesirable consequences, even though we support the predominance of the regulations.

If you take away only one thing from my testimony, let it be that privacy and secrecy can be two sides of the same coin. As you consider any privacy regulation, substitute in your mind the word "secrecy" to ensure that you fully considered the consequences of the regulation. Privacy is not exactly the same as secrecy. Privacy applies to the narrow domain of personal information. Privacy is essential to our identity and our autonomy. But within this domain of personal information, your privacy is secrecy to me and my privacy is secrecy to you. In the real world of caring for the sick, the poor, the mentally ill, the aged, and the young, the letters abound because of the duality of privacy and secrecy.

Consider the estimated 20 percent of patients who are told that death is near, yet have no memory of the news after a few days. Or the alcoholic in denial, or the school bus driver with a serious heart condition, or the parent with a genetic disease they wish to conceal from their children, or the elderly patient who is becoming forgetful, or the frightened adolescent who is pregnant or addicted, or the patient with a disease that is both contagious and stigmatizing, or the troubled patient who reveals their intent to harm themselves for another, or the child with evidence of abuse.

Only by appreciating that the favorable presumption afforded to privacy is not always correct in the complex worlds of health care can this committee appreciate that regulation can never fully substitute for discretion. It is discretion that is needed to choose between the privacy of the individual and revelations to the healing community. The sinking of the Titanic is said to have initiated the modern era of regulation, but discretion in health care will never be as easily prescribed as the number of life boats.

Consider the potentially disastrous consequences of the requirement for prior consent treatment. In a recent conversation with my mother on the occasion of her 83rd birthday, she was told that I would be testifying to this committee on privacy and health care. It was a challenge for her to understand why I needed to do this, because I hope that neither she nor any of my vulnerable patients will be confronted with yet another barrier to health care. It is because the nine pages proposed as a model of what patients need to understand in other to consent will be incomprehensible to those most in need. It is because it is incomprehensible to me that we would jeopardize the delicate task of building trust between the physician and patient by requiring a legal contract before the relationship has even begun.

What message does prior consent send to our patients who have impaired vision, hearing, or literacy? How will prior consent help or even work in life's transitions from childhood to adulthood, from independence to dependence, from competency to incompetency? How many patients will forsake evidenced-based medicine in favor of supplements and anecdotal remedies because of prior consent? How many children will not be immunized because of the barrier of the prior consent? And what will become of our dream to share other preventive information with all providers for the benefit of all our patients?

In the transition to a world of prior consent, how will patients make appointments, get answers to their questions over the phone or by e-mail, get new prescriptions, or get old prescriptions refilled?

In a world after prior consent, how will we help those who ill-advisedly revoke their consent? How will we process their bills and do peer review or even take care of them?

Another conundrum resulting from the attempt to regulate discretion is the minimum standard. The phrase, "reasonable efforts to limit the use of health information," will likely consume yet more precious resources in the possibly futile task in interpreting the definition of the use. What will the minimum necessary standard mean for teaching, for coordination of care, for cross coverage, or even consultation? And for those of us charged with creating an electronic medical record, how in this century will we ever program the rules of discretion implied by the minimum necessary standard?

In conclusion I suggest that public disclosure of privacy policies is reasonable, but the burden of prior consent is not. I suggest that allowing clinical discretion in matters of privacy is reasonable, but the burden of the minimum necessary standard is not.

Thank you for your attention.

[The prepared statement of John Melski follows:]

PREPARED STATEMENT OF JOHN MELSKI, MEDICAL DIRECTOR OF INFORMATICS, MARSHFIELD CLINIC

On behalf of Marshfield Clinic, I am pleased to have the opportunity to submit comments on the final rule adopting standards for the privacy of individually identifiable health information ("final privacy rule") published in the Federal Register on December 28, 2000. I commend you for holding this hearing and believe that Secretary Thompson should be applauded for seeking public input on the rule. Our internal analysis of the final rule suggests that patient care will be compromised significantly if this rule is implemented. In this testimony I will identify the problems that we have found and suggest remedies that may be applied.

The Marshfield Clinic is the largest private group medical practice in Wisconsin and one of the largest in the United States, with 603 physicians, 4,546 additional employees, and 1.6 million annual patient encounters. A not-for-profit corporation, the Marshfield Clinic system includes a major diagnostic treatment center, a research facility, a reference laboratory and 39 regional centers located in northern, central and western Wisconsin. Patients from every state in the nation plus patients from every county in Wisconsin were seen within the system in the last fiscal year. Security Health Plan of Wisconsin, a not-for-profit health maintenance organization, is a wholly owned subsidiary of the Marshfield Clinic and provides financing for health care services for almost 120,000 members throughout northern, central and western Wisconsin. During the last three decades, Marshfield Clinic has funded and installed a sophisticated electronic medical record which now contains years of historical data, including diagnoses, procedures, test results, medications, immunizations, alert events, outcome measurements, and demographics. Marshfield Clinic's 39 regional centers are linked by common information systems. Our physicians have stated that one of the greatest advantages of the electronic record is that they can quickly review their patient's care at other Marshfield facilities so that they can easily use the knowledge gained by their colleagues to provide the best possible care. Easy access to previous diagnostic test results avoids duplicate ordering of lab and radiology tests. Marshfield Clinic has invested significant time and resources to build a state-of-the-art electronic medical record system to better serve patients through accessible, high quality health care, research, and education. We presently put 2.5% of revenue into the operation and maintenance of the Clinic's information system, a cost for FY 2001 that works out to $22,073 per physician. We believe that if this rule is implemented our annual operational costs may increase significantly, in addition to the start up costs of implementation. We do not believe that these new costs would add any benefit to patient care.

Marshfield Clinic is committed to protecting patient privacy and confidentiality. We support the administrative simplification goals of the Health Insurance Portability and Accountability Act ("HIPAA") to reduce the administrative costs of providing health care. However, in analyzing the impact of the final privacy rule, our overriding consideration is the best interest of our patients. Certain provisions of

this final rule are incongruent with Marshfield Clinic's mission of serving patients through accessible, high quality health care, research and education. We do believe it is possible to balance the goals of protecting the confidentiality of patient information, while also allowing health care professionals to obtain the necessary information to coordinate patient care. We anticipate that the costs associated with compliance with this rule will substantially exceed HHS' estimates.

We have spent a great deal of time and resources to gain a working knowledge of this extremely complex rule—both in its proposed and final forms—and have kept an accounting of our internal costs, which are not insignificant. We have also identified problems in the final privacy rule that are simply unworkable and could seriously disrupt patient access to health care. We believe that the final privacy rule, as it is now written, may impede effective and accurate treatment, curtail preventative health care measures, and impose compliance costs that are completely antithetical to HIPAA's administrative simplification goals.

We will focus our comments on two key areas of concern: the prior consent requirement and the minimum necessary standard. We also summarize other issues that betray inconsistencies in the rulemaking process.

Prior Consent for Treatment, Payment and Health Care Operations

Section 164.506 of the final privacy rule requires health care providers to obtain a patient's written consent prior to using or disclosing protected health information to carry out treatment, payment, or health care operations. The consent form must refer the patient to the provider's notice of privacy practices (as required by section 164.520) for a more complete description of such uses and disclosures and it must state that the patient has the right to review the notice prior to signing the consent.

We are deeply concerned about the potential impact of this provision on our ability to deliver health care to patients. Although we submitted comments on the proposed privacy rule, we did not have an opportunity to comment on this major new provision because it was not in the proposed rule. In fact, in the Preamble to the proposed rule, the Department of Health and Human Services ("HHS") went to great lengths to explain why a consent requirement was unworkable and therefore rejected.[1] In that regard, we strongly support HHS' original approach. We question whether HHS's deviation from its previously stated intent can be supported under the Administrative Procedures Act. As now codified, the consent and authorization provisions in the final privacy rule raise serious procedural and practical issues that were not subject to prior public comment.

The prior consent requirement as promulgated in the final rule may unintentionally compromise the delivery of health care in the following ways:

- We will not be able to use patient information to schedule appointments, send appointment reminder letters, answer questions about treatment or medications when patients call, or conduct similar ongoing treatment and health care operations activities until we have a signed consent from every patient on file. We do not currently obtain consents for the use or disclosure of patient information for these purposes and are not required to do so by Wisconsin law. We do obtain consent prior to the release of records outside our system.
- Physicians may not be able to order a prescription and pharmacists may not be able to fill or refill a prescription without a prior written consent from the patient. This could be especially harmful to our elderly and disabled patients who often send a relative or neighbor to pick up their prescriptions. This requirement may disrupt care for many of our elderly patients who are "snow birds" when they call from other states to refill their prescriptions. For some patients this may be a mere inconvenience but for others the prior consent requirement may prove dangerous. We do not currently obtain consents for the use or disclosure of patient information for these purposes and are not required to do so by Wisconsin law.

---

[1] See Preamble to the proposed privacy rule, Section 164.506(a), page 59940, Federal Register, Volume 64, No. 212. For example, HHS stated that:

"Our proposal [to permit covered entities to use and disclose protected health information without individual authorization for treatment, payment purposes, and health care operations purposes] is intended to make the exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care. For individuals, health care treatment and payment are the core functions of the health care system. This is what they expect their health information will be used for when they seek medical care and present their proof of insurance to the provider. Consistent with this expectation, we considered requiring a separate individual authorization for every use or disclosure of information but rejected such an approach because it would not be realistic in an increasingly integrated health care system. For example, a requirement for separate patient authorization for each routine referral could impair care, by delaying consultation and referral, as well as payment."

- Marshfield Clinic has developed innovative preventative health care measures such as an immunization registry (Regional Early Childhood Immunization Network or "RECIN"). RECIN is a computer program that allows the sharing of immunization information between and among providers and public health departments. RECIN allows providers to have electronic access to a child's immunization history including any alerts or reactions to immunizations. Such access minimizes the possibility of over-immunization and potentially severe allergic reactions. Equally important, access to this information allows public health personnel to target children who have not been immunized. As a consequence of this program, Marshfield Clinic and concerned public agencies have been able to increase childhood immunization rates from 67% to 92% in Wood County alone. We hope for similar results throughout the region, but these will never be achieved under the constraints of the final privacy rule. Although Wisconsin law does not require prior consent for the release of immunization records, Marshfield Clinic has implemented a process to permit parents to decline to have their children participate in the RECIN registry and to receive immunization reminder letters. To comply with the final privacy rule, it appears that we will have to have a signed consent on file (that permits the use or disclosure of patient information for treatment, payment, or health care operations) from every parent before providers may use or disclose that parent's child's immunization information in RECIN. Although section 164.512 states that a written consent (or authorization or opportunity for the individual to agree or object) is not required for uses and disclosures for public health activities, this exception is limited to disclosures to and uses by a public health authority. If the use or disclosure of preventative health data falls within the definitions of "treatment" or "health care operations," prior written consent must be obtained. This requirement may actually harm patients rather than protect them and impede the achievement of the federal Healthy People 2010 objective 14-26, which has as its target the enrollment of 95% of children under age 6 in population based immunization registries.

Implementation of the prior consent requirement will be an administrative burden for the following reasons:

- We will have to obtain a one-time consent from patients to use or disclose their health information for treatment, payment, or health care operations purposes. While implementing this requirement in hospitals may be readily achievable (since hospitals typically obtain an admitting consent from patients), most group medical practices do not have a comparable process for obtaining this type of consent. We wonder when and where patients would sign such a consent document? To achieve 100% compliance with this requirement the Marshfield Clinic would be compelled to obtain signatures from patients who come to the Clinic from every state in the nation. It might also be necessary to re-configure patient flow processes to assure that all patient consents are captured uniformly. An alternative to implementing an admitting-type consent would be to amend existing consent forms to include the use or disclosure of patient information for treatment, payment, or health care operations. This would involve the time-consuming task of taking an inventory of the consent forms we currently use and amending these forms to comply with the consent requirements of the final privacy rule.
- We will have to develop a consent form and notice for patients. The notice requirements of the final privacy rule will require many pages of information about how we use and disclose patient information (for example, the model notice developed by the American Hospital Association is 9 pages long). The consent and notice will have to be written in terms sufficiently simple to be comprehensible to our patients, a task which may be impossible due to the complexity and sheer volume of the notice (it has taken our physicians and legal staff months to interpret these provisions). We will have to explain the consent and notice to each patient. We wonder who will explain these forms to our patients? We suspect that we will need to hire and train informed consent counselors who must staff our regional centers on a full time basis. Explaining the meaning and significance of the consent document may add as much as 30 minutes to the duration of each new patient visit. Will this time be reimbursable? We see several hundred new patients every day many of which come through urgent care centers. Our providers already face time constraints in obtaining consents for treatment and explaining the attendant risks. The length and complexity of this notice will ensure that our medical assistants and appointment coordinators will not be able to explain it to patients in addition to their normal responsibilities. Moreover, due to the length and complexity of the notice and in direct contradiction to the purpose of the notice requirement, it seems unlikely that patients

will actually be able to make an informed decision. The notice will have to be made available to every patient before consent for the use or disclosure of patient information for treatment, payment, or health care operations may be obtained.

Our estimate of the direct cost of this requirement:

350,000 unique patient per year @ 0.50 Hr/Patient = 175,000 hours
which is equivalent to 103 Full time employees at 1700 hours per year
103 FTES @ $25,000/EMPLOYEE = $2,575,000 in direct personnel costs to gather consents in the first year.

We are uncertain about the indirect costs associated with producing, distributing, and tracking consents. Children and other patients in legal guardian arrangements are included in our patient population but we remain uncertain about the additional complexity this will impose.

- The notice will have to be changed, reprinted, and staff retrained whenever we change our privacy practices. We will have to inform patients about how they may obtain a revised notice. All of these mandates will require us to devote enormous time and resources to develop an implementation process.
- The consent must be signed, kept on file and tracked. We will need to develop a system to track consents to determine whether we may use or disclose patient information for treatment, payment or health care operations purposes and to ensure that patients are not approached to sign a consent more than once. We will need to develop new information systems to coordinate the implementation and tracking of consents and notices with other requirements imposed by the final privacy rule such as authorizations and disclosures. The Marshfield Clinic presently tracks all authorized disclosures, but only a small amount of this information is tracked electronically. We also maintain an electronic log of every instance when a medical record is accessed. It is operationally very challenging to program accurate use categorizations for every instance of access. The software engineering involved in tracking all disclosures will require new fields and data capture, vastly expanding the storage volume of each record. This requirement will significantly add to the capitalization requirements and annual operating costs of our information system.
- A consent for uses and disclosures to carry out treatment, payment, or health care operations must state that the patient has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance upon the consent. What happens if a patient gives permission for treatment but subsequently revokes his or her consent? Consider the following circumstance: a patient signs a consent, and then undergoes surgery; a complication occurs; the patient hires a lawyer; the lawyer requests all medical records, and sends an authorization that revokes all prior consents and authorizations. We have the following questions: May we send the patient's insurance company a bill for the services? May we do peer review? What if the patient was seen for heart palpitations, and revokes his consent after the service was provided? Shortly thereafter, the patient is brought to the emergency room in congestive heart failure. May we look at the previous records? Will we have to remove the patient's information from our all of electronic files to ensure that the information is not used for treatment, payment, or health care operations purposes?
- A single patient encounter may produce data in multiple information systems. A purge of the patient's health information from the electronic files in these systems would require a file-by-file manual process. This would also result in throwing our billing books out of balance. A report of number of patients seen, charges and revenues generated, etc. would be in error. Lack of accurate information may cause us to violate existing requirements for Medicare reimbursement and accreditation agencies.
- Some of our electronic files do not readily support removal of data. How will we be able to prevent use of the patient's information in these files after a patient has revoked consent? To add to the confusion, what if a patient revokes consent to use or disclose only part of his/her health information? A full or partial revocation will impact our peer review activities thereby interfering with our quality improvement and quality assessment activities. All our staff rely upon accessing patient information electronically. It is unlikely that our staff would understand all of the exception steps that would be required to deal with patients who refused to sign the consent. Clinic costs to handle appointments, documentation, and billing in a fully manual mode for patients would run $30-100 per encounter. Clearly the Clinic would prefer not to refuse service to people who do not sign the consent. In some rural Wisconsin counties, all physicians are members of the Marshfield Clinic. How would these people receive care?

- The lack of adequate transition rules for the prior consent requirement raises the possibility of severe disruptions in the delivery of health care to patients in April 2003. In two years, a health care provider will not be able to use or disclose patient information for treatment, payment, or health care operations without a signed consent form on file. That consent form must state that permission was given for the use or disclosure of information for treatment, payment, or health care operations. Our existing consent forms do not address these in specific terms. Logistically, it will be impossible to have a consent on file for all of our patients by the compliance date.

Even for an entity like Marshfield Clinic with an integrated health care system and sophisticated electronic medical record, the implementation costs associated with the prior consent requirement will be enormous. The start-up costs for compliance with the regulation will increase our ongoing overhead. For example, the single task of reviewing and analyzing the final privacy rule over a 2 month period has cost the Marshfield Clinic approximately $15,000 in personnel time. Rather than going toward patient care, preventative health care measures, or quality improvement, these costs will go toward compliance with administrative burdens imposed by the final privacy rule that do not improve the confidentiality of medical information and perhaps detract from patient care. For these reasons, we urge HHS to eliminate the prior consent requirement from the final privacy rule.

The Minimum Necessary Standard

Sections 164.502(b) and 164.514(d) require that, when using or disclosing protected health information or when requesting protected health information from another covered entity, covered entities (i.e., providers, plans and clearinghouses) make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary standard does not apply to disclosures to or requests by a health care provider for treatment. As "protected health information" is defined in section 164.501, this standard applies to patient information in any form (oral or written) or medium (paper or electronic).

We are pleased that the minimum necessary standard does not apply to disclosures to a health care provider for treatment purposes. This represents a significant improvement over the initial approach of the proposed rule. Nevertheless, we need clarification as to whether the minimum necessary standard applies to the *use* of patient information by a health care provider for treatment purposes. In section 164.501 of the final privacy rule, "use" is defined as "the sharing, employment, application, utilization, examination, or analysis of such [i.e., individually identifiable health information] information within an entity that maintains such information." We are gravely concerned that this exception appears to exclude uses of patient information for treatment purposes. Limiting the ability of teams of health professionals and trainees (such as residents and medical students) within an integrated health care system to use a patient's entire medical record could be disruptive and dangerous. Similarly, oral communications between health care professionals in the course of treatment are an important part of the coordination of care. The omission of critical information that could result from the application of the minimum necessary standard to such uses and communications could place the patient in jeopardy. We strongly urge HHS to exclude both disclosures and uses by providers for treatment from the minimum necessary standard.

Another concern we have with the minimum necessary standard is the lack of an objective standard to guide providers in their implementation efforts. We do not know what constitutes "reasonable efforts" to limit information to the minimum necessary. In the Preamble to the final privacy rule, HHS explains that "the policies and procedures [to limit access] must be based on reasonable determinations regarding the persons or classes of persons who require protected health information, and the nature of the health information they require, consistent with their job responsibilities. For example, a hospital could implement a policy that permitted nurses access to all protected health information of patients in their ward while they are on duty." Consistent with its commitment to protect patient privacy, Marshfield Clinic has long had confidentiality policies limiting access to patient information based on job responsibilities. Access to patients' electronic medical records is granted to a staff member only if their job responsibilities require this access. Because it is not possible to know which patients a staff member needs to access, they have access to all patients' records. (In compliance with Wisconsin law, some information relating to psych patients has further restrictions to access.) The Clinic follows a need-to-know policy, and it is a violation of the policy to access a patient's record without a need to know. All electronic accesses are electronically logged and violators of Clinic policy have been terminated from employment at the Clinic. Since

Marshfield Clinic has such a system, will a policy approach to limit access, without accompanying electronic restrictions, be deemed "reasonable" under the final privacy rule? Our electronic system is not set up to handle electronic restrictions and adding this capability to our system would be cost prohibitive. In addition, some employees presently perform multiple functions and may have access to the patient record during one activity but would be denied it during another. Many providers see patients in multiple sites on a changing schedule. Their staff either travel with them or are reassigned at their site. It is not unusual for one employee to work in two or three locations within the course of a week, and sometimes in the course on one day. They may even change job roles—for example a medical assistant filling in as a receptionist, appointment coordinator or phlebotomist. Modifying their ability to access patient information as they move will require additional security staff, verification by a manager to confirm that it needs to be done. This will also result in delays, as an employee arrives at a new location and cannot do their job until their rights are approved and changed in the computer system. In such situations will we have to restructure the tasks or hire additional personnel? The reconfiguration of administrative processes is not accounted for in HHS cost estimates for implementing the privacy regulation. We request that HHS provide an objective standard to guide providers in their implementation efforts with the minimum necessary standard.

We also see problems in the rule for psychotherapy notes that contemplates use of the note only by the originator of the note or for use in training programs. This does not represent the way mental health care is delivered in integrated systems of care: by a team of professionals, often in multi-disciplinary staffing arrangements (e.g., psychiatrist, psychologist, social worker, psychiatric nurse). These would not likely be training programs; these individuals are generally all on staff. This provision also does not seem to allow use by the psychiatrist on call, a very dangerous proposition. For use by others on the treatment team who are not the originator of the note, we would need the patient's authorization (which the patient may refuse to provide and we may not condition treatment on provision of an authorization).

We have identified numerous problems in other provisions of the final privacy rule. However, we chose to focus on the prior consent requirement and the minimum necessary standard to highlight the most serious consequences that will result from implementation of the final privacy rule. We anticipate that the reworking of all business associate contracts, the development of internal policies and procedures to comply with the privacy regulation, and the training of all employees in privacy policies will be costly, time consuming, and administratively complex.

In summary, we believe that the final privacy rule, as presently written, threatens to disrupt patient care and unnecessarily divert time and resources from Marshfield Clinic's foremost priority of treating patients. We therefore respectfully request that Congress direct HHS to reevaluate the final privacy rule and revise the troublesome provisions.

Thank you for considering our views.

Mr. BILIRAKIS. Thank you very much, Dr. Melski.

Dr. Appelbaum.

STATEMENT OF PAUL APPELBAUM

Mr. APPELBAUM. Mr. Chairman, I am Paul Appelbaum, M.D., vice president of and testifying on behalf of the American Psychiatric Association, a medical specialty society representing more than 40,000 psychiatric physicians nationwide. I am professor and chair of the Department of Psychiatry at the University of Massachusetts Medical School where I treat patients and oversee our department's biomedical and health services research.

Chairman Bilirakis, and Ranking Member Brown, I would like to thank you for the opportunity to testify today. We recognize that there is still work to be done with the HIPAA regulations to improve their protection of patient privacy. At the same time, we believe that any delay in implementation is contrary to the health needs of the American people. Regrettably, the centrality of confidentiality to high-quality health care is often overlooked. Some patients refrain from seeking medical care or drop out of treatment in order to avoid the risk of disclosure of their records, and some

patients simply will not provide the full information necessary for successful treatment.

Patient privacy is particularly critical in ensuring high-quality psychiatric care. Accordingly, the APA recommends that at the close of comment period, the administration not delay implementation but, rather, use its regulatory authority to respond appropriately to comments. And we suggest this notwithstanding our concerns detailed below.

In our view, the final privacy regulations are an important step toward protecting patient privacy, because the regulations ensure, among other positive provisions, non-preemption of more privacy protective State laws:

A rule that psychotherapists' notes may not be disclosed without the patient's specific authorization.

A requirement that the entire medical record not be used in cases where a portion of the record will suffice; that is, the "minimum amount necessary" requirement.

However, it is clear that in several places, these regulations fall short of adequate protection for patient privacy. Let me offer you four examples, and there are others cited in our written testimony.

First, holders of medical information should be required to obtained meaningful consent from patients before their medical record can be disclosed for treatment, payment, or health care operations. In this regard, we are concerned about blanket consent at the time of entry into a health plan. This blanket consent means a patient is authorizing subsequent disclosures of personal information without knowing the type of information to be disclosed or who will receive the information.

Second, significantly narrower definition of the information that may be released for payment purposes is needed. Excessive demands by payers for access to patients' medical information, which often include requests for entire patient records for which there is no legitimate need, should not be allowed. We ought to bring the interested parties together to work out an objective standard for the necessary information.

Third, additional protections consistent with the Supreme Court's Jaffee v. Redmond decision for mental health and other particularly sensitive medical record information are essential. Language needs to be added to extend the regulations, psychotherapy privacy protections to all psychiatric information, including information that is part of the patient's medical record. Currently only psychotherapy notes outside the record would receive special protection under these regulations.

Fourth, we also want all Americans to be free from unreasonable police access to their most personal medical record information. Under these regulations law enforcement agents could simply issue written demands to doctors, hospitals and insurance companies to obtain patient records without judicial review. A separate provision would allow for the release of medical record information any time the police are trying to identify a suspect. This broad exception would allow computerized medical records to be sifted through by the police looking for matches for blood or other traits.

We believe that the same constitutional protections, that is a Fourth Amendment probable cause standard including independent

judicial review for all requests, should apply to a person's medical history as applies to their household possessions.

We also have concerns about the administrative burdens placed on practitioners. At a minimum, similar to small health plans, small physician offices should be allowed 36 months for compliance to spread the costs over a longer period of time, and responsibility for violation of the regulations by business associates clearly needs to be rethought.

In conclusion, we believe the privacy regulations are very much needed, but at the same time believe that some provisions are inadequate to protect our patients. Yet our biggest concern is that certain parties who are disappointed at how protective these regulations are of patient privacy will, in support of their own interests, be arguing for surrendering many of the protections that patients have just gained.

To preclude diminution of medical record privacy protections, we recommend that the Secretary use his regulatory authority after the close of the comment period to work with the stakeholders' representatives to find an appropriate solution to the problems identified.

We thank you for this opportunity to testify, and we look forward to working with the committee on medical records privacy issues.

[The prepared statement of Paul Appelbaum follows:]

PREPARED STATEMENT OF PAUL APPELBAUM, VICE PRESIDENT, AMERICAN PSYCHIATRIC ASSOCIATION

Mr. Chairman, I am Paul Appelbaum, M.D., Vice President of and testifying on behalf of the American Psychiatric Association (APA) a medical specialty society representing more than 40,000 psychiatric physicians nationwide. I am Professor and Chair of the Department of Psychiatry at the University of Massachusetts Medical School. I frequently treat patients, and I also oversee the Department's biomedical and health services research including medical records based research.

Chairman Bilirakis, and Ranking Member Brown I would like to thank you for the opportunity to testify today. I would also like to thank the members of the Committee, Representatives Greenwood and Waxman, who have focused the Committee's attention on medical records privacy.

Privacy and particularly medical records privacy is an issue all Americans are concerned about. I thank you for your continued commitment to protecting medical records privacy and for holding this hearing on the recently released Medical Privacy Regulation.

We recognize there is still work to be done to overcome implementation obstacles to achieve compliance if these regulations are to appropriately serve the needs of the American people. At the same time please know that any delay in the implementation date is contrary to the health needs of the American people.

Regrettably, it is often overlooked that confidentiality is an essential element of high quality health care. Some patients refrain from seeking medical care or drop out of treatment in order to avoid any risk of disclosure of their records. And some patients simply will not provide the full information necessary for successful treatment. Patient privacy is particularly critical in ensuring high quality psychiatric care.

Both the Surgeon General's Report on Mental Health and the U.S. Supreme Court's *Jaffee v. Redmond* decision conclude that privacy is an essential requisite for effective mental health care. The Surgeon General's Report concluded that "people's willingness to seek help is contingent to the comments received on their confidence that personal revelations of mental distress will not be disclosed without their consent." And in Jaffee, the Court held that "Effective psychotherapy depends upon an atmosphere of confidence and trust . . . For this reason the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment."

Accordingly, the APA recommends at the close of the comment period the Administration move forward with the publication of the regulations and not delay the im-

plementation date but rather use their regulatory authority to respond appropriately in the public interest and to protect the privacy of the medical record. And we suggest this notwithstanding our concerns that we believe changes in the provisions on mental health records are critically needed to ensure the delivery of effective mental health care, or other comments that may be submitted.

The regulations should be implemented, then after the comments have been reviewed by HHS the "stakeholders" can be brought together, and we can secure the necessary stronger protections to advance patient privacy which we as physicians believe that our patients and our families need.

While, the APA is concerned that some provisions are inadequate to protect patients and that some administrative requirements are unnecessarily complex. The final privacy regulation is an important first step toward protecting patient privacy because the regulation ensures:

- the general rule of non-preemption of more privacy protective state laws
- a higher level authorization is required for any use or disclosure of psychotherapy notes, and most importantly psychotherapy notes may not be disclosed without the patient's specific authorization
- the requirement that the entire medical record not be used in cases where a portion of the record will suffice, i.e. the "minimum amount necessary" requirement. Physicians can cite this provision when dealing with unreasonable health plan requests for information.
- the requirement that an entity must notify enrollees no less than once every three years about the availability of the notice of privacy policies and how to obtain a copy of it
- extension, in many circumstances, of federal "common rule" research protections to privately funded research
- the right to request restrictions on uses or disclosures of health information (such as requesting that information not be shared with a particular individual)
- the right to request that communications from the provider or plan be made in a certain way (such as prohibiting phone calls to an individual's home)
- the right to inspect and copy one's own health information with the exception of psychotherapy notes and when the access is reasonably likely to endanger the life and physical safety of the individual or another person
- the right of patients to be provided documentation on who has had access to this information and the right to request amendment to the record if it contains incorrect information

Health care plans, and clearinghouses must be required to obtain an individual's meaningful consent before their medical record can be disclosed for treatment, payment, or other health care operations it should not be limited only to providers. Patients should be able to choose who will see their medical records. In this regard, we are concerned about blanket consent at the time of entry into a health plan. This blanket consent means a patient is authorizing subsequent disclosures of personal information without knowing the type of information allowed to be disclosed, or who can receive this information. While the regulations allow the patient to revoke this consent, the regulations do not protect the patient from being dismissed from the plan for doing so. The patient should have the ability to revoke the consent at any time. The APA feels the rule does not adequately provide this patient protection.

Currently, most hospitals ask patients to sign a consent form for treatment and payment. Excessive demands by payers for access to patients' medical information, which often amount to requests for entire patient records, should not be allowed. The demands routinely include information for which there is no legitimate need for payment purposes. Significantly narrower definition of the information that may be released for payment purposes is needed to protect patient privacy. We need to bring the interested parties together to work out an objective standard for the information that is needed, not a subjective standard.

Patients should have the right to consent to—or refuse—participation in disease management programs. In addition, an individual's enrollment or costs should not be affected if he or she declines to participate in a plan's disease management program. We oppose any disclosures of health information for disease management activities without the coordination and cooperation of the individual's physician. Yet, there is no such requirement in the final rule. We believe "disease management" needs to be defined narrowly, in order to prevent inappropriate use and disclosure (for example for marketing purposes) of health information without the patient's consent.The APA is concerned about the disclosure of medical records for judicial and administrative proceedings. Patients will lose some existing privacy protections because the current practice of hospitals and doctors, generally requiring patient consent and/or notice before disclosure, will change as a result of the regulation. Pa-

tients' ability to decide when their medical record information will be disclosed outside the health system will be reduced.

For example, currently when hospitals or doctors receive a request for a medical record from an attorney for civil and administrative purposes, they will generally not disclose medical records information without notice to the patient and/or the patient's consent. But the new regulation would allow providers to disclose medical records information to attorneys who write a letter "certifying that the . . . information requested concerns a litigant to the proceeding and that the health condition of such litigant is at issue". These procedures provide no check on attorneys' behavior in requesting records of marginal relevance to a case or for the purpose of embarrassing or intimidating opposing parties. Once the information is disclosed, the damage is done; post hoc remedies cannot restore parties' privacy.

The APA is very concerned about a marketing and fundraising loophole that exists in the regulation. A patient's authorization is not needed to make a marketing communication to a patient if: it occurs face-to-face; it concerns products or services of nominal value; and it concerns the health-related products and services of the covered entity or of a third party and meets marketing communication requirements. For example, a marketer could knock on the door of a pregnant woman and try to sell her a product or service. Under the fundraising loophole a covered entity may use or disclose patient's demographic information and dates of health care to a business associate or to an institutionally related foundation, without a patient's authorization. We are aware the covered entity must include in any fundraising materials it sends to a patient a description of how the patient may opt out of receiving any further fundraising communication. However, the APA maintains that the patient should be asked for consent before the fundraising communication is sent. For example, a commercial fundraising organization for a health facility could use confidential information about a Governor being a patient at that facility without the Governor's consent for use in their fundraising. The APA is particularly concerned about the need for sensitivity with psychiatric patient's names. Commercial fundraisers should not be allowed to take advantage of patients especially those with mental illness.

We strongly believe that personal health information should never be shared for the purposes of marketing or fundraising without the patient's informed consent and are disappointed that the rule only permits an ex post facto withdrawal of consent after the marketing and fundraising damage has occurred. There is an easy solution, merely require the fundraising endeavors to have a patient consent (opt in) before the activity occurred rather than the regulation's authorizing the patient to opt out of any further fundraising endeavors.

Additional protections consistent with the Supreme Court's *Jaffee v. Redmond* decision for mental health and other particularly sensitive medical record information are essential. Without such additions the protections essential for effective mental health care will be lost. This is necessary until all medical records enjoy a level of protection so that no additional protections are needed for psychiatric or other sensitive information. In fact, the U.S. Supreme Court recognized the special status of mental health information in its 1996 *Jaffee v. Redmond* decision and ruled that additional protections are essential for the effective treatment of mental disorders.

APA believes that the rule allows for the use and disclosure of far too much information without the patient's consent. We also believe that language needs to be added to clarify that the amendment's privacy protections cover treatment modalities broader than psychotherapy (and indeed virtually all psychiatric information) and also cover information that is part of the patient's medical record. The regulations change the current standard of practice relevant to the psychotherapy documentation. There is a new requirement for keeping a second set of records, which most psychiatrists do not now do, and which will result in increased time, difficulty, and cost associated with record keeping.

We also want all Americans to be free from unreasonable police access to their most personal medical record information. The Administration's proposal falls short in this area. Under these regulations law enforcement agents would simply issue written demands to doctors, hospitals and insurance companies to obtain patient records, without needing a judge to review the assertions. We are also very concerned by the separate provision that would allow for the release of medical record information anytime the police are trying to identify a suspect. This broad exception would allow computerized medical records to be sifted through by police to seek matches for blood, DNA or other health traits. In addition, the provision that allows disclosure on the basis of an administrative subpoena or summons, without independent judicial review, is particularly troublesome.

We believe that the same constitutional protections (a Fourth Amendment probable cause standard including independent judicial review for all requests) should apply to a person's medical history as applies to their household possessions.

The business associate provisions of the proposed regulation result in overly broad physician liability, and the regulations also need to be reconsidered in light of the need to limit the administrative burden on physicians who practice independently or in small practices. The rule identifies most health care related entities other than physicians, providers, health plans, and health data clearinghouses as "business partners" of physicians, which could only be held to the confidentiality standards of the regulation through contracts with the covered entities, such as physicians. In essence this enormous regulatory framework will be achieved largely through the inappropriate liability placed upon physicians.

A covered entity will have a new duty to mitigate any known harmful effects of a violation of the rule by a business associates. This duty may, in effect, compel covered entities to continue to monitor activities of business anyway. It is not clear if a psychiatrist, for example, could be held accountable for prohibited activity by its business associate, if the psychiatrist **should have known** of the prohibition. For purposes of the rule, actions relating to protected health information of an individual undertaken by a business associate are considered to be actions of the covered entity. Therefore even though covered entities may avoid sanctions for violations by business associates if they discover the violation and take the required steps to address the wrongdoing, they may be vulnerable to a negligence action. APA believes these provisions present the potential for overly broad liability for physicians who, themselves, are complying with the regulation's requirements.

It is not unreasonable to expect that some additional burdens will fall on physicians as part of efforts to increase patient privacy. However, the level of administrative burden currently contained in these regulations is not equitably distributed. Particularly important is expanding the concept of scalability so that the administrative burden on physicians in solo or small practices will be manageable, taking into consideration their limited resources and staffing. As I discussed, the regulatory framework of this regulation relies too heavily on physician liability. If indeed it is the framework by the Secretary that is enacted through regulation or through congressional action, we could not support providing individuals with a private right of action.

The special rules in the specialized government functions are overly broad and do not provide adequate procedural protections for patients. Except in very narrow circumstances the consent of the individual should be the rule for the use and disclosure of governmental employees' medical records information. We also note that intelligence agencies and the State Department are not even required to publish a rule, subject to public comment, defining the scope and circumstances of their access to medical records. Particularly objectionable are the provisions allowing broad access without patient consent for use and disclosure of medical records of Foreign Service personnel and their families.

The APA believes the estimated costs imposed on small psychiatrist's offices for the first year of $3,703 and consecutive years of $2,026 seem unrealistically low. Psychiatrists will experience significantly higher costs and will have a heavy administrative burden, such as getting satisfactory assurances from a business associate through a written contract, keeping psychotherapy notes separate and locked away from the rest of the psychiatric record, and providing written notice of their privacy practices to their patients. Similar to small health plans, small physician offices should be allowed to have 36 months for compliance to spread the cost over a longer period of time.

A clarification is needed on the privacy official provision. For example, can a psychiatrist who does not have any staff serve as the privacy official? If a privacy official makes a mistake will only the privacy official be liable?

In conclusion, we believe the privacy regulations are very much needed but at the same time believe some provisions are inadequate to protect our patients. Yet, our gravest concern is that certain parties that were disappointed at how protective these regulations are of patient privacy will, in support of their own interests, be arguing for surrendering many of the protections that patients have just gained. In order to insure that interested stakeholders' regulatory comments do not diminish medical record privacy protections we recommend that the Secretary not only receive all interested stakeholders' (such as insurers, providers, health care clearinghouses, and consumer groups) comments, but use his regulatory authority after the close of the comment period to work with the stakeholders' representatives to find solutions. Moreover, the regulation's preamble says "the privacy standards are consistent with the objective of reducing the administrative costs of providing and paying for health care".

We of course encourage the Administration to stand firm on these issues and support strong protection of medical record privacy. Secretary Thompson has stated that he would "put strong and effective health privacy protection into effect as quickly as possible." We hope the Administration keeps their promise to the American people.

We thank you for this opportunity to testify, and we look forward to working with the Committee on medical records privacy issues.

Mr. BILIRAKIS. Thank you very much, Dr. Appelbaum.

To introduce the next witness to us on behalf of himself and also on behalf of his Congressman Pat Kennedy, the Chair recognizes Mr. Brown.

Mr. BROWN. Thank you, Mr. Chairman.

Congressman Kennedy was up here a moment ago and wanted to stay and introduce Carlos Ortiz, who also I have worked with for some years on prescription drug issues. And Congressman Kennedy had to go to another hearing, but he wanted to extend his wishes to you and thanks for joining us.

STATEMENT OF CARLOS R. ORTIZ

Mr. ORTIZ. Thank you, Congressman Brown.

Mr. Chairman and other members of the subcommittee, my name is Carlos Ortiz, and I am director of government relations for CVS Pharmacy, and I am also a pharmacist. I very much appreciate this opportunity to testify before the subcommittee today on the impact of the recent Federal privacy regulations on community pharmacies and the patients we serve.

As the largest private pharmacy provider in the Nation, CVS operates almost 4,100 pharmacies in 32 States and through our Internet CVS.com in all 50 States. In 2001, we will provide an estimated 325 million prescriptions to approximately 40 million patients. CVS operates 278 pharmacies in the districts of the subcommittees—districts of the members of the subcommittee.

CVS wants to reiterate our commitment to strong Federal standards with State preemption to protect the privacy of medical records. CVS believes that the new Federal privacy standards that are developed, whether through statute or regulation, must ensure that patients can obtain prescription services in a timely and efficient manner.

Unfortunately some aspects of the new final rules are unworkable and will have unintended consequences for patients and pharmacies. We support Secretary Thompson's action to seek further comments on the final regulation. Many provisions in the final rule were not included in the proposed rule and thus not fully vetted.

I think most people understandably want to have their prescriptions filled as quickly as possible. No one wants to spend more time in a pharmacy than they need to when they are not feeling well. And it is important to start drug therapy as soon as possible. However, a new requirement in the final rule which was not in the proposed rule would require direct treatment providers such as pharmacists to obtain signed written consent from the patient before they can use the patient's information to provide treatment or seek payment. That is, pharmacies cannot fill or begin the process of filling prescriptions before the patient's signed written consent is on file. This will increase waiting times, inconvenience patients, and negatively impact the quality of care.

Currently no State law requires pharmacies to obtain written consent from patients, so this requirement represents a fundamental change in how patients interact with the pharmacies and how pharmacies interact with patients. We believe in the concept of statutory authorization; that is, the presentation by the patient of a prescription to the pharmacy demonstrates sufficient consent for the pharmacy to use the patient's information to provide the medication and bill for payment. We assume the patient—if the patient did not want the prescription filled or refilled, he or she would not take it to that pharmacy or have the physician call it in to that pharmacy.

You should know that approximately 40 percent of all prescriptions are dropped off and picked up by someone other than the patient. Problems will result when the patient's representative shows up at the pharmacy and finds that because a signed written consent was not on file, they have to go back to the patient's home, have the consent signed, and then drive back to the pharmacy and wait and have the prescription filled.

I would venture that this is a prescription for chaos. We believe it will cost us at least $60 million to communicate in writing with our 40 million patients about the need to have a prior consent on file prior to the effective date of the final rule if they are to go on and continue to receive prescription service uninterrupted.

Additionally, the oral communications, having the prior consent apply to oral communications, provides very certain barriers to the ability of the pharmacist to provide information concerning nonprescription medication. Imagine a customer coming in, who is not a regular pharmacy patient, indicating to you that they are diabetic and would like a sugar-free cough syrup, and you have to tell them, sorry, before I can take that information and use it and provide you with information concerning a proper cough syrup for your use, I am going to need a written consent from you because you are not one of my regular pharmacy patients.

At a time of pharmacist and staffing shortages, these added costs will go toward patient—will not go toward patient care, quality improvement or innovation.

CVS also believes that the new comprehensive privacy laws should preempt State privacy law. Community retail pharmacies are operating thousands of stores in multiple States. Given the significant length and scope of privacy notices and consents required, the cost of exchanging and reissuing them every time a State law or regulation is exchanged is staggering when you are dealing with millions of patients.

In conclusion, let me iterate our strong commitment to Federal standards with State preemption to protect the privacy of medical records. However, we believe that the new written prior consent requirement, especially for the billions of prescriptions filled annually by community retail pharmacies, presents significant operational, logistical and patient care challenges. The unintended consequences of this requirement will result in patient frustration and longer waiting times at the pharmacy counter.

Thank you for the opportunity.

[The prepared statement of Carlos R. Ortiz follows:]

PREPARED STATEMENT OF CARLOS ORTIZ, DIRECTOR OF GOVERNMENT AFFAIRS, CVS PHARMACY

Mr. Chairman and Members of the Subcommittee. My name is Carlos Ortiz and I am Director of Government Relations for CVS Pharmacy Corporation, based in Woonsocket, Rhode Island. I am also a pharmacist and have been since 1966. I very much appreciate the opportunity to testify before the subcommittee today on the issue of medical records privacy and the impact of the recent final Federal privacy regulations on community pharmacies and the patients that we serve.

As the largest private pharmacy provider in the nation, CVS operates almost 4,100 community pharmacies in 32 states and through CVS.com in all 50 states. In 2001, we will provide an estimated 325 million prescriptions to over 60 million patients. CVS operates 278 pharmacies in the districts of this subcommittee's members.

CVS is committed to safeguarding the privacy of patient medical records. Currently, in most states, licensed pharmacists must abide by patient privacy standards specified in state pharmacy practice acts, state board of pharmacy regulations, and other state laws. In addition to these requirements, retail pharmacies commonly require employees to comply with stringent patient privacy policies.

CVS wants to reiterate our commitment to strong, Federal standards, with state preemption, to protect the privacy of medical records. CVS believes that any new Federal privacy standards that are developed, whether through statute or regulation, must strike the appropriate balance of assuring that any new protections do not outweigh the ability of patients to obtain prescription services in a timely and efficient manner.

Impact on Patients and Pharmacies of Prior Written Consent Requirement

Unfortunately, these new final regulations, if implemented in their current form, are unworkable and will have unintended consequences for community retail pharmacies and the patients that we serve. We support Secretary Thompson's action to seek further comments on the final regulation, because we believe that there were many provisions in the final rule that were not included in the proposed rule, and thus not fully vetted.

Most people want to have their prescriptions filled as quickly as possible. That is understandable. No one wants to spend more time in a pharmacy than they need to when they are not feeling well, and it's important to start drug therapy as soon as possible.

A new requirement in the final rule, which was not in the proposed rule, would require direct treatment providers, such as pharmacies, to obtain signed written consent from the patient *before* they can use the patient's information to provide treatment or seek payment. That is, pharmacies cannot fill or even begin the process of filling prescriptions before the patient's signed, written consent is on file. Even HHS said that such a prior consent requirement was unworkable, and rejected its use in the original proposed rule.

Requiring pharmacies to obtain signed written consent from patients before we can provide prescription services will increase waiting times, inconvenience patients, and negatively impact the quality of care. Currently, no state law requires pharmacies to obtain written consent from patients, so this requirement represents a fundamental change in how patients interact with pharmacies *and* how pharmacies interact with patients.

We believe that the presentation by the patient of a prescription to the pharmacy demonstrates sufficient consent for the pharmacy to use the patient's information to provide that medication and subsequently bill for payment. We assume if the patient did not want the prescription filled (or refilled), he or she would not take it to the pharmacy. If the patient did not want the physician to call the prescription into a particular pharmacy, he or she wouldn't ask the physician to do so. That, we believe, represents sufficient consent.

Moreover, we do not see how this prior written consent requirement creates any additional privacy protections for patients, as long as the pharmacy's use of the information is limited to that which is allowed under the definitions of treatment, payment, and health care operations.

Yet, the requirement for prior written consent was included in the final rule, without any opportunity for public comment. We do not believe that the full implications and unintended consequences of this inclusion are yet understood by patients.

Approximately 40% of all prescriptions are dropped off and picked up by someone other than the patient. As a result, you can see the potential for problems being created when the patient's representative shows up at a pharmacy and finds that, because a signed written consent is not on file, they have to go back to the patient's

home, have the consent signed, and then drive back to the pharmacy and wait to have the prescription filled. This could be especially burdensome for those individuals that live in rural areas, and those who live in urban areas and don't have easy access to transportation.

For example, parents with sick children, and others, such as elderly, disabled, and other homebound individuals, would have to come to the pharmacy to sign a consent or send someone on their behalf to obtain a consent and take it back home for signature and then back to the pharmacy before the pharmacist may fill or refill a prescription. So, a mother, who had expected to pick up the prescription that was phoned in earlier by the doctor, will now find that she has to wait for her child's medication.

The homebound elder without any nearby relatives would have to find someone to go to the pharmacy and get the consent form, bring it back to the patient for their signature, then return to the pharmacy with the consent and the prescriptions, and wait for the prescriptions to be filled.

Furthermore, if the written prior consent requirement goes into effect, patients with active prescription refills on file would first have to go to the pharmacy and provide a signed, written consent before we could refill the prescription. How will we communicate to those patients that they need to go into the pharmacy and sign a written consent form before we can refill their prescription? Should we wait until they call in their refill or until they show up at the pharmacy counter expecting their prescription to be refilled in a timely manner?

This is a prescription for chaos. I would venture that we will try and communicate ahead of time, in anticipation of the effective date of the final rule, if the final rule contains the requirement for prior written consent, probably in writing. Yet even the simple act of trying to communicate in writing with 60 million patients will be a difficult and very expensive proposition, probably in excess of $60 million.

Because the final regulation also extends privacy protections to "oral communications" between pharmacists and patients, the pharmacist cannot talk to the patient about their health condition in order to recommend a possible over-the-counter product, until the patient signs a written consent at the pharmacy.

Millions of Americans patronize pharmacies everyday to seek advice from pharmacists about non-prescription medicines. How can we logistically obtain all these consents, commit this information to paper, and then recommend an appropriate medication in a timely manner? This interference may cause customers to start going to other outlets that also sell OTCs, such as convenience stores that are not direct treatment providers. We think this is bad medicine. Consumers should have the benefit of consulting with a pharmacist without having the hassle of having to sign a written consent before they are able to do so.

The cost of compliance with this massive regulation is itself staggering. Those costs will not go toward patient care, quality improvement, or innovation. Rather, pharmacies, at a time of pharmacist and staffing shortages, will be required to implement these time-consuming regulations at the expense of patient care.

Strong Federal Privacy Protections with Preemption of State Laws

CVS also believes that new comprehensive Federal standards should preempt state privacy laws. Community retail pharmacies, operating thousands of chain pharmacies in multiple states, need one Federal standard rather than 50 different standards to interpret. Subsequently, conflicts between federal and state law could be virtually impossible for health care providers to resolve on a patient-by-patient basis.

This final regulation does not preempt many state-based privacy laws. In fact, states can and likely will enact a "patchwork" of privacy laws, creating a situation where providers will have to determine themselves which is stronger, state based laws, Federal regulations, or court cases relating to patient privacy that might be relevant in particular situations. Moreover, the final rule does not provide for the Secretary to issue guidance to providers concerning which state laws are contrary to and more restrictive than the rule, or to regularly update the guidance.

As a result, community pharmacies will have to develop a process to regularly monitor which law, regulation, or court case should be applied, and have to update their "privacy notices" accordingly. Given the significant length and scope of the privacy notices and consents required under the rule, the cost of changing and reissuing them every time a state law or regulation is changed is staggering. This is especially true when you are providing millions of prescriptions each year and operating in multiple states.

While we understand that only a new Federal statute can preempt state law, not Federal regulations, we believe that Federal policymakers should take action this year to preempt state laws and create nationally uniform Federal privacy protec-

tions. At the very least, we urge that HHS be required to provide guidance in the regulations and in their implementation that will provide certainty to covered entities as to which state laws are "more stringent" than the HHS regulations.

Conclusion

CVS wants to reiterate our commitment to strong, Federal standards, with state preemption, to protect the privacy of medical records. We are seriously concerned about this new written prior consent requirement in the final HHS regulations for direct treatment providers, which did not appear in the proposed rule, and for which public comment has not been allowed or the implications for patients adequately assessed.

We believe that this new written prior consent requirement, especially for the billions of prescriptions filled annually by community retail pharmacies, presents significant operational, logistical, and patient care challenges, and that the unintended consequences of this requirement will result in patient frustration and longer waiting times at the pharmacy counter.

We have joined with other organizations in asking Secretary Thompson to delay the April 14, 2001 effective date of the rule and to work with us, as well as other affected parties, to determine how we might best address these and other important implementation issues. We want to work with Members of this Committee and the Congress to assure that reasonable privacy protections result from this process, and that patients' access to efficient, effective pharmacy services remains. Thank you for the opportunity to submit these comments for the record.

Mr. BILIRAKIS. Thank you.

Ms. Goldman.

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

Ms. GOLDMAN. Thank you, Mr. Chairman and members of the committee, for the opportunity to testify today. No one has ever said that they can't hear me, but having the mike, I guess, helps.

I wanted to thank you for inviting me here to testify today, and I know we don't have much time, so I wanted to say that while I have heard so many things here today that are distressing in terms of what the actual regulation says, and I think there is some misinterpretation and inaccuracies, our full statement does try to anticipate some of those statements and to correct them.

And I want to suggest at the outset that this is not a new process. For those of you who have worked on this issue, we have been at it for over a decade. Congress has been at this since the early 1990's, if not before. Many of the issues that are in the final regulation were incorporated into bills that were introduced on a bipartisan basis by many members of this committee and in the Senate as well, so there has been a great opportunity to look at this.

The comment period on the regulation was extended in response to requests by industry groups and consumer groups, and then there was a 10-month fact-finding process where HHS tried to develop a workable and a strong rule. And I say that at the end, consumer advocates and providers got some of the things we asked for, and health plans and others got some of the things they asked for. Nobody got everything. But there was an attempt within the constraints that HIPAA set on the administration to craft a strong privacy rule that was workable.

Protecting privacy we now know is not only good for individuals, it is good for health care generally. And many, I think, of the leaders in the community are already developing privacy and security standards in their systems.

The regulation is not perfect. There is no question some of the areas where we think it is weak are again areas where there were constraints imposed by the Congress in 1996, that it can only directly cover certain entities, that it only directly covers information in certain contexts. There is limited enforcement, limited liability.

We did ask that there be an expansion in the scope of the regulation. Provider groups were very clear. Doctors and others said that they wanted a consent requirement because that is currently the status quo. There is not an—I don't ever go to the doctor where I am not asked to sign a consent form. I have never enrolled in a health plan where I am not asked to sign a consent form. So that is the status quo. And health care providers were adamant that that not be rolled back.

In terms of the major points that I want to make today, we are urging the administration to go forward with the April 14 effective date of this regulation. There has been adequate time over the last few months, and there will be over the next month, to look at where there may be some concerns, where there may be real barriers to implementation. And where they exist, and where they can be shown on a case-by-case basis, and not, you know, about the hyperbole and extreme concerns, but where we know there are going to be barriers, we urge Secretary Thompson to make the modifications necessary to permit compliance, to issue guidance where that would be helpful to allay some of the fears that have arisen around the implementation of the regulation. He has full legal authority to do that. We urge him to use it and to not further delay this regulation.

A lot of the opposition, as I said, I think are based on inaccuracies and misstatements about this regulation, and it gives us concern that the efforts around delay are really to try to delay the regulation indefinitely. We have been at this for over a decade now. While many say they want privacy and they care about privacy, we have never really seen a true commitment to moving forward in this area. Many other industries have moved forward to put privacy protections in place and have worked closely with consumer groups and others in the financial area, in the communications area, in the video rental area, where it was critical to engender consumer trust and confidence that privacy protections were essential to get people to fully participate.

E-commerce is a big issue right now, and the No. 1 barrier to people fully participating is concern about their privacy. But it appears that the health care industry has not moved forward with that same urgency to allay public concern and to calm people.

We have seen major problems. We have seen at the University of Washington a major breach in security because there weren't rules in place saying what folks needed to do in order to adequately protect data. These privacy regulations, while not perfect, and while not comprehensive, will create tremendous uniformity. It will certainly, to an industry that needs to start to build privacy protections in, to say, here is the way to do it. It will give some calm assurance to the public, who is very concerned about sharing information and are withdrawing from full participation in their own care. People are afraid to get genetic tests because of how the information might be misused. They are afraid to go online to get access

to information or services because of how the information might be misused.

We would hope that the Secretary would take into account what some of the real concerns are. I think that there are some issues that can be addressed with his legal authority, and we would urge him to do that. But where, again, there is hyperbole or misstatements, we would urge the Secretary as well as this committee to take a look at those and hopefully to set the record straight. I hope this hearing is an opportunity to do that.

[The prepared statement of Janlori Goldman follows:]

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

Members of the House Committee on Energy and Commerce, Subcommittee on Health: As the Director of the Health Privacy Project at Georgetown University's Institute for Health Care Research and Policy, I very much appreciate the invitation to testify before you today on the final medical privacy regulation.

INTRODUCTION

The medical privacy regulation issued by the Department of Health and Human Services (HHS) on December 28, 2000, is a milestone in federal law. It is the first—and only—federal law to protect the privacy of medical information in the hands of private health care providers and health plans. This regulation was initially scheduled to go into effect on February 26, 2001, but its effective date was changed due to the unfortunate failure of HHS to officially transmit the regulation to Congress. We urge the Administration and the Congress to ensure that this regulation goes into effect, as now scheduled, on April 14, 2001.

After the regulation goes into effect, if covered entities have real and legitimate implementation concerns that guidance from HHS cannot address, the Secretary of HHS has the legal authority to make certain modifications to the regulation, as necessary to permit compliance. We are fully available to support Secretary Thompson should such modifications become necessary, and we look forward to working with him as we move forward. What we would not support, and, indeed, would vigorously oppose, is any action by HHS or Congress that would further delay the effective date or roll back the regulation.

As you hear testimony today, we urge you to look at the actual language of the regulation as it is written and at HHS' intent as expressed in the preamble. It is essential that we not be swayed by distortions and exaggerations that we fear are part of a strategy to not only delay, but also to undermine the regulation. We believe that some in the health care industry are engaged in a campaign to do just that. Fortunately, not all health-related entities share that goal. Most notable are the trade associations and individual companies that know that protecting privacy is good for business, and support the regulation and the time line for implementing it.

Our testimony today addresses: the importance of protecting privacy in the health care arena; the genesis of the health privacy regulation; why HHS should not further delay implementation of the regulation; a brief summary of the final regulation; the major areas of contention; the myths that are being propagated about the final regulation and the facts; a rebuttal of the industry's cost concerns; and our recommendations to Congress.

OVERVIEW OF THE HEALTH PRIVACY PROJECT

The Health Privacy Project's mission is to press for strong, workable privacy protections in the health care arena, with the goal of promoting increased access to care and improved quality of care. The Project conducts research and analysis on a wide range of health privacy issues. Recent Project publications include: *Best Principles for Health Privacy* (1999), which reflects the common ground achieved by a working group of diverse health care stakeholders; *The State of Health Privacy* (1999), the only comprehensive compilation of state health privacy statutes; *Privacy and Confidentiality in Health Research* (2000), commissioned by the National Bioethics Advisory Commission; *Privacy and Health Websites,* which found that the privacy policies and practices of 19 out of 21 sites were inadequate and misleading; and "Virtually Exposed: Privacy and E-Health" (2000), published in *Health Affairs.*

In addition, the Project staffs the Consumer Coalition for Health Privacy, comprised of over 100 major disability rights, disease, labor, and consumer advocates as well as health care provider groups. The Coalition's Steering Committee includes AARP, American Nurses Association, Bazelon Center for Mental Health Law, National Association of People with AIDS, Genetic Alliance, National Multiple Sclerosis Society, and National Partnership for Women & Families.

PRIVACY IS A CENTRAL VALUE IN HEALTH CARE

Americans are increasingly concerned about the loss of privacy in everyday life, and especially about their health information. The lack of privacy has led people to withdraw from full participation in their own health care because they are afraid that their most sensitive health records will fall into the wrong hands, leading to discrimination, loss of benefits, stigma, and unwanted exposure. One out of every six people engages in some form of privacyprotective behavior to shield herself from the misuse of health information, including withholding information, providing inaccurate information, doctorhopping 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 conducted by Princeton Survey Research Associates for the California Health Care Association, 1999)

Unfortunately, people's fears are warranted. Medical privacy breaches are reported with increasing frequency by the media. To highlight a few—

- Terri Seargent was fired from her job after her employer learned that she had been diagnosed with a genetic disorder that would require expensive treatment. Terri was a valued employee who received a positive review and a raise just before her discharge from the company. A recent EEOC investigation determined that the employer fired Terri because of her disability.
- A few months ago, a hacker downloaded medical records, health information, and social security numbers on more than 5,000 patients at the University of Washington Medical Center. The University conceded that its privacy and security safeguards were not adequate.
- Annette W. and her husband were involved in a difficult and contentious divorce. In the midst of their separation, Annette instructed her pharmacy not to disclose any of her medical information to her estranged husband. Just one day later, the pharmacist gave Annette's husband a list of all her prescription drugs. Armed with this information, her husband embarked on a campaign to label her a drug user. He sent information to friends and family, to the Department of Motor Vehicles, and threatened to have her children taken away.
- bYears ago, Ben Walker and his wife came to Congress to tell their story. Ben had worked for the FBI for 30 years, but was forced into early retirement after his employer learned that he had sought mental health treatment. The FBI got hold of Ben's prescription drug records when the Bureau was investigating his therapist for fraud. In turn, the FBI targeted Ben as an unfit employee and stripped him of many of his duties, even though he was later found fit for employment. Ben and his wife testified that he would never have sought treatment had he believed his medical records would be used against him.

In the absence of a federal health privacy law, these people suffered job loss, loss of dignity, discrimination, and stigma. And had they acted on their fears and withdrawn from full participation in their own care—as nearly 20% of people do—they would have put themselves at risk for undiagnosed and untreated conditions. In the absence of a law, people have faced the untenable choice of shielding themselves from unwanted exposure or sharing openly with their health care providers.

THE GENESIS OF THE REGULATION

The new federal health privacy regulation is a major victory for all health care consumers. In fact, each one of us will benefit from these rules in some way, from more reliable data for research and outcomes analysis, to greater uniformity and certainty for health care institutions seeking to develop privacy safeguards as they modernize their information systems. The rules represent a significant and decisive step toward restoring public trust in our nation's health care system. Not only is it the most sweeping privacy law in U.S. history, it begins to fill the most troubling vacuum in federal law. The regulation sets in place a sorely needed framework and a baseline on which to build. Much of the regulation's unfinished business is due to the legal constraints imposed on HHS by Congress in its delegation of authority in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). At this juncture, it is imperative that Congress act to plug the gaps and strengthen the weaknesses in the rule.

In fact, it was a Republican Congress in 1996 that imposed on HHS the legal duty to issue a health privacy regulation. Representatives of health care consumer groups, health plans, and health providers all reached a consensus in 1996 that the movement toward an electronically based health care system should not go forward without adequate federal protections in place for the confidentiality and privacy of health information. HIPAA reflects this consensus. It sets a schedule for adopting and implementing not only the standards for electronic transactions involving health information, but also for establishing privacy protections for health information.

Many privacy bills were introduced after HIPAA passed in 1996. Some were bipartisan; others were not. Some were favored by consumer advocates, others by health plans. Numerous hearings were held in both the House and Senate, but not a single bill saw a mark-up. Achieving legislative consensus on health privacy rules is not a simple task. Congress' failure to meet the 3-year deadline set in HIPAA triggered the requirement for HHS to promulgate rules in this area by 2000.

Pursuant to its mandate, HHS issued draft regulations in November 1999. In response to requests from industry representatives and consumer advocates, the Department extended the formal comment period to allow sufficient time to respond to the proposal. Of the 52,000 comments eventually submitted, more than half came from consumers and their representatives. After the comment period closed, HHS spent 10 months engaged in extensive fact finding to respond to comments and concerns before it released the final regulation.

The final regulation incorporates a number of the key changes sought by consumer groups as well as many of the changes urged by health care providers, health plans, clearinghouses, researchers, and others operating in the health care arena. From the text of the regulation itself, it appears HHS was striving to craft a strong *and* workable privacy law.

It is important to note that the privacy rule is one of three regulations mandated in the section of HIPAA known as "Administrative Simplification." The other rules address establishing uniform transaction standards for health care and security rules to safeguard the data. Congress intended this package of regulations to be implemented together so that privacy and security measures are built in as information systems and practices are standardized. The policy goal was to assure the public that, as their most sensitive personal information was being computerized and adapted to be shared instantly and cheaply, enforceable privacy rules would be implemented up front. The final transactions standards went into effect last fall, triggering a 24-month implementation period. The security regulations are expected to be released by HHS this spring.

WE URGE HHS NOT TO FURTHER DELAY THIS IMPORTANT PRIVACY REGULATION

We strongly support maintaining the current effective date of the final privacy regulation. HIPAA mandated that regulations governing the privacy of health information be promulgated by February 2000. These privacy standards are long overdue, already have been thoroughly debated, and should be put into effect as scheduled.

The rule-making procedure up to this point has been lengthy, thorough, and orderly. Scores of HHS employees spent almost a year reviewing, analyzing, and crafting responses to the comments that the agency received on this rule. The thoroughness with which HHS considered these comments is reflected by the fact that almost 200 pages of the preamble to the final regulation are devoted to summarizing and responding to these comments.

Overall, the final product of these extensive rule-making procedures is a balanced regulation. HHS made many significant changes to accommodate the concerns of the major stakeholders. For instance, in response to concerns from the health care industry, the requirements of the "business partner" provisions were substantially relaxed. The requirement of a third party beneficiary clause in a business associate contract was eliminated as was the provision that would have held a covered entity liable for violations of its business associates that it should have known about. Now, they are merely liable for violations they actually knew about. Restrictions on marketing and fundraising activities were also substantially relaxed after vigorous lobbying by the health care industry. In response to the comments of health providers and health care consumers, authorization requirements were tightened. In sum, although no one group of stakeholders received everything that it requested, the comments of all major stakeholders were taken into account in crafting the final rule.

If there are legitimate implementation issues that cannot be remedied through the issuance of guidance by HHS, HIPAA expressly provides a mechanism for resolving these difficulties *after* the privacy regulation becomes effective. Under Sec-

tion 262 of HIPAA (adding Section 1174 to the Social Security Act), the Secretary has the authority to modify the privacy standards during the first 12 months after the standard is adopted (*i.e.*, becomes effective) when such modification "is necessary in order to permit compliance with the standard." Thus, HIPAA anticipates and provides a statutory mechanism for resolving implementation problems after the regulation becomes effective.

At this critical juncture, it is time to move forward and devote our energy, time, and resources toward implementing the final regulation, rather than wasting precious resources debating whether the regulation should even take effect. Every day more progress is made toward electronically storing and transmitting health information. As Congress recognized in 1996, it is irresponsible to allow these changes to go into effect without having adequate privacy and security protections in place.

SUMMARY OF THE FINAL REGULATION

Key provisions of the health privacy regulation are highlighted below. A more detailed, comprehensive summary of the rule can be found at our website, www.healthprivacy.org.

- **Scope:** The regulation applies to all health plans and clearinghouses (entities that process and transmit claims data) and to health care providers that transmit claims-type information in electronic form. It covers identifiable health information in electronic and paper records as well as oral communications. Due to the constraints imposed by HIPAA, the law does not directly cover employers, life insurers, pharmaceutical companies, and others. Instead, the rule establishes a chain of trust requirement, binding entities that receive identifiable health information from a covered entity to a contractual arrangement.
- **Access:** People have the right to see, copy, and amend their own medical records. Most states do not currently grant people such broad rights.
- **Limits on Disclosure:** The regulation restricts access to and disclosure of health information. Of particular importance to patients and providers, health care providers must obtain patient consent for disclosures relating to treatment, payment, and health care operations. We support this approach. However, we believe the provisions on marketing and fundraising are fundamentally flawed in allowing "one free pass" before first giving people the chance to opt-out of receiving such commercial communications.
- **Employers:** Group health plans are barred from disclosing "protected health information" to employers except for specific functions related to providing and paying for health care. Employers must establish a firewall between the health care division and those employees who make decisions about employment. The rules are a powerful new tool to stop workplace discrimination. However, due to constraints imposed by HIPAA, employers that collect health information directly from employees (and not in their capacity as providers, plans or clearinghouses) fall outside the scope of the privacy rule. Only Congress can close this gap.
- **Law Enforcement:** Health care providers and plans are prohibited from releasing patient data to federal, state, or local law enforcement without some form of legal process, including a warrant, court order or administrative subpoena. There is a broad consensus among consumer organizations and the health care industry that HHS should have established stronger legal process requirements. The Health Privacy Project had argued to HHS that it should require a higher Fourth-Amendment standard and review by a neutral magistrate.
- **Research:** All research, whether publicly or privately funded, must be overseen by either an Institutional Review Board (IRB) or privacy board if the researcher seeks a waiver of informed consent.
- **Penalties:** Health care providers, health plans, and clearinghouses are subject to civil and criminal penalties (up to $250,000/year and 10 years in jail) for violating the law. The Office for Civil Rights at HHS is charged with overseeing the law and imposing penalties where appropriate. But HIPAA constrained the Secretary from including a federal private right of action for individuals to sue for violations of the law. Congress should act to give people the ability to seek redress directly if their rights are violated.
- **Preemption:** As required in HIPAA, the federal regulation does not preempt or override stronger state law. Instead, the rules establish a baseline of protections, above which states may go to better protect their citizens. A 1999 report on state laws issued by the Health Privacy Project demonstrated that such a baseline is sorely needed.

MAJOR AREAS OF CONTENTION

As expected, the final rule has been the subject of much criticism from some of the entities that will be covered by it. In this section we address those criticisms that reflect policy differences between HHS and the covered entities—policy differences that were aired, debated, and resolved as part of this rule's lengthy rule-making process. In the next section we address the campaign of misinformation that opponents of the final regulation are waging in an effort to further delay its effective date.

Consent requirement for health care providers (Section 164.506)

We are pleased that the final rule requires that a health care provider obtain a patient's consent before using or disclosing protected health care information. We are disappointed that the consent requirement was not extended to other covered entities, such as health plans.

As a general rule, requiring patient consent prior to use or 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 the use and disclosure of their information; and
- define an "initial moment" in which patients can raise questions about privacy concerns and learn more about options available to them.

See Best Principles for Health Privacy, a Report of the Health Privacy Working Group, at 22.

Patients should be encouraged to be active participants in their own health care—and obtaining an individual's consent is an integral piece of that picture. Accordingly, we believe that health plans should also be required to obtain an individual's consent prior to using or disclosing health information for treatment, payment, and health care operations purposes. This is particularly true in light of the breadth of activities encompassed in the definition of "health care operations," which expanded considerably from the proposed rule.

Some industry groups have claimed that the public comment process was circumvented because the final rule governing authorization and consent varied significantly from the proposed provision on this topic. *See, e.g.,* Testimony of American Benefits Council before the Senate Committee on Health, Education, Labor, and Pensions at 7 (February 8, 2001); Testimony of the American Hospital Association before the Senate Committee on Health, Education, Labor, and Pensions at 9 (February 8, 2001). However, the Secretary's actions were well within the standard of appropriate rule-making behavior. Under the proposed rule, authorization or consent for treatment, payment, and health care operations purposes would not have been required. After explaining the basis for this proposed approach, the Secretary "invit[ed] comments on whether other approaches to protecting individuals' health information would be more effective." 64 Fed. Reg. at 59941. The Secretary received some 52,000 comments on the proposed regulation, many of them from health care providers and consumer groups addressing the lack of any requirement for patient authorization for these purposes. Based on these comments, the Secretary strengthened the standard. This is how rule-making is supposed to occur: the agency makes a proposal, the public comments on it, the agency considers those comments and then modifies the rule, if necessary, in response to those comments. There was no circumvention of the rule-making process in establishing consent standards.

In essence, the industry's argument boils down to a policy difference with HHS over the best approach to consent. Those views were aired thoroughly and then rejected by HHS as it crafted the final regulation.

At least one organization has stated that the final consent requirement could, in fact, lead to actual harm of individuals seeking health care. They have expressed concern that treatment might be delayed when "individuals seek[] medical care or services in those unavoidable instances where no consent form has been obtained." Testimony of American Benefits Council at 8. However, the final privacy regulation has taken this possibility into account. Section 164.506(a)(3) provides that a health care provider may without prior consent use or disclose protected health information in emergency treatment situations and in circumstances where the provider is unable to obtain prior consent due to substantial barriers to communication with the patient.

Some pharmacy groups have expressed concern that the consent requirement would substantially interfere with their current method of operation. Frequently, prescriptions are phoned or faxed into pharmacists by doctors. The pharmacist then uses the prescription information in order to have the medication ready when the patient or someone acting on behalf of the patient arrives to pick it up. We recognize

that requiring a consent to be on file in advance of using a prescription for treatment purposes would interfere with these current business practices. We believe, however, that HHS can remedy this problem quite easily, either by issuing guidance that a pharmacist in such a situation would be considered to have an indirect treatment relationship with the patient or by making a minor change in the definition of "indirect treatment relationship" found in Section 164.501. However, this potential need to "fine tune" the regulation does not justify delaying the effective date.

Business associates (Sections 164.502(e) and 164.504 (e))

We strongly support the requirement that covered entities receive satisfactory assurance that their business associates will properly safeguard protected health information before either disclosing this information or allowing a business associate to receive protected health information on their behalf. Absent such a requirement, covered entities could easily circumvent the privacy regulation merely by contracting out their business functions.

Ideally, a health privacy law or regulation would impose restrictions directly on all of those who receive protected health information, including the agents and contractors of health care providers and health plans. Unlike health care providers, these downstream users and processors often do not have an ethical obligation to maintain patient confidentiality. We recognize, however, that HHS was unable to directly cover these organizations due to the Secretary's limited authority under HIPAA. Regulating the agents and contractors of covered entities indirectly, through the covered entities, makes sense in these circumstances. This is particularly true since many covered entities already enter into some form of contract with their business partners.

Some covered entities have protested that it is not fair to hold them accountable for the actions of others. However, this regulatory scheme is not a departure from traditional contractor/agency principles under which a contractor may be held responsible for its agents' actions. Furthermore, HHS took the fairness argument into account and weakened this provision in the final rule by limiting a covered entity's liability to circumstances where the covered entity actually knew of a material breach of the contract of the business partner and failed to act.

Other organizations have complained that business associate contracts would be complex and result in significant time and resource burdens, and would require the writing or re-writing of many new contracts. We note at the outset that having contracts in place specifying what agents are permitted to do with sensitive health information just makes good business sense. Additionally, the implementation specifications for business associate contracts are clear and straightforward and should not result in complex contracts. In order to reduce any administrative burden, covered entities are free to develop standard contracts or standard addenda to existing contracts.

Again, as with the final rule's approach to consent, the business associate concept was thoroughly debated during the rule-making process and there is no reason to reopen that debate.

Minimum necessary standard (Sections 164.502(b) and 164.514(d))

We support the general standard that a covered entity must make reasonable efforts to limit protected health information to the minimum amount necessary to accomplish the intended purpose when using or disclosing protected health information or when requesting such information from another covered entity. We are particularly pleased that the minimization requirement extends to payment and health care operations.

The final rule significantly modified the proposed minimum necessary standard and the related implementation specifications. In some ways, the rule has been improved, such as subjecting the *requests* of covered entities for health information to the minimum necessary standard. See Section 164.514(d)(4). However, in many other ways the standard is still lacking because it does not apply to a broad enough category of uses and disclosures of health information.

Probably the most controversial aspect of the minimum necessary standard is the method in which it applies to protected health information that is being used or disclosed for treatment purposes. The minimum necessary standard *does not* apply to information that is *disclosed* to a health care provider for treatment purposes. See Section 164.502(b)(2)(i). In contrast, the minimum standard *does* apply to health information that is being *used* for treatment. We believe that the minimum necessary standard should apply to *both* uses and disclosures of protected health information for treatment purposes.

Under the structure of the final rule, a covered entity could adhere to this requirement by fashioning general policies that specify when and who should have ac-

cess to medical information for treatment purposes. *See* Section 164.514(d)(3). For instance, a hospital might have a policy that would permit a treating physician access to a patient's entire medical record, but would limit a nurse's aide's access.

The establishment of policies governing the amount of information accessible within a covered entity will become even more important as the health care delivery system continues to move toward computerization of medical records. As a practical matter, records in this format may be readily accessible to a wide range of personnel within the covered entity. Thus, it is imperative that a covered entity have policies that limit uses of health information to the minimum amount necessary.

Oral communications (Section 160.103, definition of "health information")

Much criticism of the final rule has focused on its applicability to oral communications. Some of this criticism has reached hyperbolic proportions. For example, Blue Cross and Blue Shield charges that "new sound-proof walls and offices may need to be built in health care facilities." *See* Testimony of Blue Cross and Blue Shield Association before the Senate Committee on Health, Education, Labor, and Pensions at 7 (February 8, 2001). The American Hospital Association raises the specter of doctors not being able to talk to patients who share a hospital room with another patient "for fear of running afoul of HIPAA's many prohibitions." See Testimony of the American Hospital Association before the Senate Committee on Health, Education, Labor, and Pensions at 10 (February 8, 2001).

Health care professionals, and the hospitals in which they work, should take reasonable steps to make sure that conversations about one patient are not overheard by others. The regulation, though, merely requires covered entities to "reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards." *See* Section 164.530(c)(2). Screens or curtains often separate patients from one another in hospital rooms to protect the privacy of patients. Health care professionals can and should modulate their voices so that private conversations can take place. This is true whether the conversation takes place in the patient's room or in the hallways, corridors, or elevators.

We believe that HHS has the authority under HIPAA to regulate a broad range of health information in any format, including oral communications, and we strongly support this approach. Not only does HHS have the authority to protect health information in any format, it *should* protect this information.

At the outset, protecting only health information in electronic format would leave a vast amount of health information unprotected by federal law. Furthermore, limiting coverage to only health information that at some point had been electronically maintained or transmitted would be impractical and unenforceable. Health information often changes format—it can start out as oral, then be written and then be stored electronically. It would be an administrative nightmare to try to discern what information in any particular health record had at some point been electronically stored or transmitted. Additionally, if there were an improper disclosure, it would be terribly difficult, if not impossible, to prove that the information disclosed had at some point been in electronic format.

Leaving health information in paper and oral format outside the bounds of the privacy regulation may actually induce covered entities to retain paper record-keeping and filing systems in order to avoid regulation. This would be contrary to the goals of the administrative simplification provisions of HIPAA, which are intended to encourage the development of an electronic health care information system. Moreover, if oral communications were excluded from the regulation, covered entities could circumvent this regulation merely by reading aloud or orally telling someone what is contained in a computer or paper record.

MAJOR DISTORTIONS ABOUT THE PRIVACY REGULATION

Some in the health care industry oppose aspects of the privacy rule and the time line for implementing it, and are waging a "chicken-little-the-sky-is-falling" campaign to delay and weaken it. In this section we rebut the major myths and inaccuracies about the final rule.

Myth #1: The regulation will "jeopardize the quality and timeliness of patient care" and "drive a wedge between individuals and their care providers."

Sources: "HIPAA's Privacy Standards: Driving a Wedge Between Patients and the Health Field," by Marilou M. King, attorney representing the American Hospital Association (page 1); Testimony of Blue Cross and Blue Shield Association before the Senate Committee on Health, Education, Labor, and Pensions at 11 (February 8, 2001)("This standard . . . could jeopardize the quality and timeliness of patient care . . .").

Fact: The regulation will improve the quality of care and the patient/professional relationship. Concerns about lack of privacy now drive a wedge between patients and their providers and impede the provision of quality care because patients withhold information, avoid asking certain questions, or fail to seek care altogether. Among other benefits, the regulation creates the opportunity for patients and their health care providers to engage in a dialogue about how their information will be used and gives patients more control over uses and disclosures. This regulation will go a long way toward promoting confidence in the privacy of medical information and in the health care system.

Myth #2: Family members and friends will no longer be able to pick up prescriptions for others at the pharmacy.

Source: "'As Craig Fuller has told me, the way it's set up right now, if you are married and you're too sick to go to the drug store, you can't send your spouse down to pick up your medicine,' [HHS Secretary] Thompson said during a National Chamber Foundation meeting March 1 in Washington, D.C." F-D-C Reports' Research Services, "Consulting NACDS," The Pink Sheet, March 5, 2001 (page 5).

Fact: The regulation explicitly provides that this common practice can continue. The regulation states that covered entities can use their professional judgment and experience with such practices so that family members, friends, and others may pick up items like filled prescriptions, medical supplies, or x-rays. See Section 164.510(b)(3).

Myth #3: The "minimum necessary" standard will disrupt communications between providers involved in treating a patient. Some charge that providers treating patients will not be able to examine the patient's entire medical record.

Sources: "The minimum necessary rules may still place artificial limits on the ability of doctors to use and disclose health information for critical treatment situations—threatening the overall quality of care." Testimony of Blue Cross and Blue Shield Association before the Senate Committee on Health, Education, Labor, and Pensions at 11 (February 8, 2001).

"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." Testimony of Blue Cross and Blue Shield Association before the Senate Committee on Health, Education, Labor, and Pensions at 11 (February 8, 2001).

"Limiting the ability of teams of health professionals, and health profession trainees, in a hospital setting to use a patient's complete medical chart or freely discuss and communicate among themselves in the course of treating patients could be disruptive and potentially dangerous." Testimony of the Healthcare Leadership Council before the Senate Committee on Health, Education, Labor, and Pensions at 4 (February 8, 2001).

Fact: The regulation explicitly exempts from the "minimum necessary" standard all disclosures to providers for treatment purposes. It also exempts all requests by health care providers for information to be used for treatment purposes. See Section 164.502(b)(2)(i). As a result, information will flow freely between and among providers involved in treatment. Provisions in the regulation that require special justification for disclosing the entire medical record **do not apply** to treatment-related disclosures because they are not subject to the minimum necessary standard in the first place.

With respect to *uses* of health care information for treatment purposes, the regulation allows the use of the entire medical record when it is specifically justified as the amount that is "reasonably necessary" to accomplish the purpose of the use. *See* Section 164.514(d)(5). A provider is only required to have a policy as to the amount of health information that is to be used: a case-by-case determination is not required or anticipated. *See* Section 164.514(d)(3). In fact, HHS states in the preamble to the regulation that HHS "expect[s] that covered entities will implement policies that allow persons involved in treatment to have access to the entire record, as needed." 65 Fed. Reg. at 82544.

Myth #4: Providers that disclose medical information for treatment purposes must meet the minimum necessary standard.

Source: "This exemption [from the minimum necessary standard] does not cover . . . 'disclosures *by*' providers." (emphasis added) Testimony of Blue Cross and Blue Shield Association before the Senate Committee on Health, Education, Labor, and Pensions at 11 (February 8, 2001).

Fact: This assertion takes the minimum necessary exemption out of context. The general rule imposes the minimum necessary standard on covered entities, including providers, when they are "disclosing protected health information." *See* Section

164.502(b)(1). The provision goes on to state: "This requirement does not apply to:...Disclosures to...a health care provider for treatment." *See* Section 164.502(b)(2). When read as a whole, it is clear that the exemption applies to disclosures *by* health care providers.

Myth #5: The regulation will impede the training of medical students, in part because the regulation will not allow medical students to see a patient's entire medical record.

Source: The Association of American Medical Colleges has "grave concerns" about "the effects of the rule on medical and health education." "The AAMC supports the proposition that medical residents and medical and nursing students, as well as other health professions students, as necessary, should have unrestricted access to medical information of their patients...—a proposition that the rule seems to recognize, peculiarly, only with respect to psychotherapy notes." Testimony of the Association of American Medical Colleges before the Senate Committee on Health, Education, Labor and Pensions at 2, 4 (February 8, 2001).

Fact: The regulation respects the important role that covered entities play in the training of medical students. It includes the following within the definition of "health care operations" found in Section 164.501: "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers." Therefore, once a provider obtains a consent, an individual's health information can be used not only for treating the patient but also for training medical students. Disclosures, for treatment purposes, to medical students providing health care services to patients would not be subject to the minimum necessary standard because such medical students would be considered "health care providers." *See* Section 160.103 (definition of "health care provider")("any other person...who furnishes...health care"). Medical students—even those not actually considered "health care providers" because they do not furnish care—would be able to review a patient's entire medical record when the covered entity makes a policy determination that the entire medical record is "reasonably necessary to achieve the purpose" of training medical students. *See* Section 164.514(d)(5).

Myth #6: The regulation is so complex it is 1,500 pages long.

Source: U.S. News & World Report (Jan. 29, 2001, page 47) refers to the regulation as "the 1,500-page doorstopper."

Fact: The text of the actual regulation only covers 32 pages in the Federal Register. The preamble that precedes the regulation covers 337 pages in the Federal Register. Over half of the preamble is devoted to summarizing and responding to the more than 52,000 comments received by HHS.

Myth #7: "Health care providers would have to keep track of everyone who received medical information from them. Patients could demand an accounting of all of these disclosures."

Source: Amitai Etzioni, "New Medical Privacy Rules Need Editing," USA Today at 13A (February 22, 2001).

Fact: This is simply not true. Providers are *not* required by this regulation to keep an accounting of anyone within their own organization who has received (or had access to) medical information. This is because the accounting provision only covers "disclosures," which are defined as the sharing of health information with someone outside of an organization. *See* Section 164.528(a) (right to accounting of disclosures) and Section 164.501 (definition of "disclosure"). Furthermore, the regulation specifically states that a provider does not have to keep account of information disclosed (*i.e.,* shared with someone outside of the organization) for treatment, payment, or health care operations. *See* Section 164.528(a)(1)(i). For example, a hospital would not have to keep track of health information sent to outside doctors providing follow-up care to patients. The result of these exclusions is that providers are required to account for only a narrow category of disclosures that primarily are *not related to health care,* such as those made to law enforcement personnel or pursuant to a request for documents in a lawsuit.

Myth #8: The regulation allows patients to demand that doctors correct their medical records.

Source: "We all would be the beneficiaries if the regulations as currently constituted were not allowed to go into effect until they are subject to an expeditious and thorough trimming and simplification...And while patients should be allowed to see their medical records and attach their comments, they should not be allowed to demand that doctors "correct" the records." Amitai Etzioni, "New Medical Privacy Rules Need Editing," *USA Today* at 13A (February 22, 2001).

Fact: There is no provision allowing patients to demand that doctors "correct" their records. An individual may request that a provider (or other covered entity)

amend his or her records and append or otherwise provide a link to the location of the amendment. *See* Section 164.526(c)(1). Amending a medical record usually does not involve actually removing information, but *adding* an amendment with the accurate data. There are several grounds under which a provider may deny such a request to amend. *See* Section 164.526(d).

Myth #9: The final regulation requires disclosures of protected health information to a variety of federal government departments and agencies.

> Source: "What has not been widely reported are the rule's new mandates requiring doctors, hospitals, and other health care providers to share patients' personal medical records with the federal government, sometimes without notice or advance warning. (See, for example, Federal Register, Vol. 65, No. 250, December 28, 2000, p. 82802, Sec. 160.310.)... Handing sensitive medical records to federal departments and agencies that are ill-equipped to protect that information is not a solution; it is inviting abuse, errors, scandal, and tragedy." Letter from Dick Armey, House Majority Leader, to Secretary Thompson (dated March 5, 2001).

Fact: The regulation *requires* covered entities to make only two types of disclosures: (1) disclosures to the individual who is the subject of the protected health information and (2) disclosures to HHS for the purpose of enforcing the regulation. *See* Section 164.502(a)(2). The regulatory section cited by Majority Leader Armey in his letter requires disclosures to HHS for compliance purposes. It restricts such disclosures to that information that is "pertinent to ascertaining compliance with [the regulation]." Without this provision, HHS would have no way of determining whether a covered entity had complied with the regulation, making enforcement of the law impossible. Moreover, HHS is limited in what it can do with health information obtained in this fashion. The regulation prohibits HHS from disclosing such information except where necessary to ascertain or enforce compliance with the regulation or as required by other law. *See* Section 160.310(c)(3). Under an executive order issued contemporaneously with the final regulation, HHS is also prohibited from using protected health information concerning an individual discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations against the individual.

The regulation does not require disclosures to any other person or entity, including to other federal agencies or departments. The regulation *permits* disclosures to government agencies only where the agency requesting or receiving the information has authority to request or receive the information through some other law. *See, e.g.,* Section 164.512(d)(1) (disclosures for health oversight activities "authorized by law").

COST CONCERNS SUPPORT THE APRIL 14 EFFECTIVE DATE

Industry opponents cite the cost of complying with the regulation as a reason to delay or weaken it.[1] We believe the costs of *not* implementing this rule on schedule far outweigh the costs of implementing it. If we, as a society, do not put federal privacy protections in place, millions more people will engage in privacy-protective behaviors—to the detriment of their own health and the integrity of research—and confidence in our health care system will continue to erode.

HHS estimates that the cost associated with implementing the privacy regulation (approximately $17 billion over ten years) will be greatly offset by the cost savings associated with implementing HIPAA's transactions standards (approximately $29 billion **saved** over ten years). If implemented together, as contemplated by Congress, consumers will benefit, health care organizations will benefit, and the health of our communities will benefit. Delay would actually be more costly for industry because it would need to redesign and retool systems a second time if privacy protections are not put in place along with the transactions standards.

Rather than spending resources on fighting this regulation, we urge the industry to work toward implementation. Some industry organizations already have urged Secretary Thompson to implement the regulation without further delay.[2] We are

---

[1] "An AHA-commissioned study, looking at hospital costs alone, found that the cost of only three key provisions of the proposed rule... could be as much as $22.5 billion over five years." Testimony of the American Hospital Association before the Senate Committee on Health, Education, Labor, and Pensions at 6 (February 8, 2001).

[2] *See, e.g.,* letters to Secretary Thompson from The Coalition for Health Information Policy (comprised of American Health Information Management Association, American Medical Informatics Association, and Center for Healthcare Information Management) (dated February 7, 2001), and Association for Electronic Health Care Transactions (AFEHCT) (comprised of a variety of organizations, including Aetna US Healthcare, IBM, Medscape, and WebMD) (dated February 2, 2001).

aware of at least one national health plan that already is beginning the process of moving forward with this regulation, and we applaud them for doing so. These groups understand that protecting privacy is good for business.

CONCLUSION

Americans should be proud of what Congress set in motion with HIPAA and with the thoughtful and deliberate way in which HHS carried out its congressional mandate. While we would have preferred that HHS make different policy judgments in several areas—most notably in the areas of law enforcement and marketing/fundraising—we do not believe these weaknesses in the final regulation warrant further delay in the effective date or a reopening of the regulation. Similarly, the policy differences that some in the industry have with HHS over some aspects of the final regulation do not warrant further delay or a reopening of the rule-making process. We do urge HHS to issue guidance on the regulation, and to rely on its legal authority to act where necessary on a case-by-case basis during the two-year implementation phase.

To improve privacy protections for consumers, Congress can intervene and pass a law that requires consumer consent before medical information can be used for marketing and fundraising purposes. Congress can also enact a law that strengthens the limits on law enforcement access to medical records. And Congress can fill in the gaps left by HIPAA by directly regulating other entities that collect and use personal health information and by equipping people with the federal right to go to court if their privacy is violated under the law.

We look forward to continued progress on health privacy. Our health care system has changed dramatically in the last few years, bringing with it both promise and perils. We have mapped the human genome, but people are afraid to get tested. The Internet can deliver cutting edge research and health care services, but people are unwilling to trust their most sensitive information in cyberspace. We will never fully reap the benefits of these astounding breakthroughs until privacy is woven into the fabric of our nation's health care system.

Mr. BILIRAKIS. Mr. Heird.

STATEMENT OF ROBERT HEIRD, SENIOR VICE PRESIDENT, ANTHEM BLUECROSS BLUESHIELD

Mr. HEIRD. Thank you, Mr. Chairman, members of the committee. I am Bob Heird, vice president of Anthem BlueCross and BlueShield, headquartered in Indianapolis, Indiana. We are also the Blue Cross and Blue Shield plan in seven other States. I am testifying today on behalf the Blue Cross and Blue Shield Association, and we appreciate this opportunity to share our views with you.

Blue Cross and Blue Shield plans agree that a basic set of clear rules is necessary to assure consumers their health care information is strictly private. For us there is no question as to whether patient records should be kept private, but only as to how.

Mr. BILIRAKIS. You are welcome to repeat that if you would like. I apologize for that.

Mr. HEIRD. I was trying to outperform the buzzers.

Our challenge is to review these rules through the eyes of our consumers. Our members demand and expect superior customer service. A key question for us is whether this rule meets those customer expectations, and we have concluded that they do no not, and that is because the rule is operationally infeasible, extremely costly, and could threaten quality improvements throughout the health care system. And because of these concerns, the need for further analysis, we are pleased Health and Human Services has provided another comment period to allow time to identify and correct those serious problems in the final regulation that could, in fact, harm consumers.

Today I would like to highlight four issues. First, our members want clear guidelines about where to direct questions and problems. Unfortunately, the final rule would layer new Federal rules on top of existing State laws and would only add more red tape and confusion for everyone. Consider, for example, an Anthem customer living in Lawrenceburg, Indiana, working in the Cincinnati/Northern Kentucky Airport, and visiting a doctor in Cincinnati, Ohio. Each of those stops are about 25 minutes apart. If there is a concern about privacy, who do they call? Do they call the regulators in the State where they live? Do they call the regulator in the State where they work where the contract was issued; where care was provided? All three? And what is HHS's role in viewing those issues? So is it really four entities that they need to contact to work those issues through?

Second, our customers want timely quality care, the kind of care that America prides itself on. The minimum necessary rule would require all of us to establish new procedures, and reorganize and redesign our operations so we are only using and disclosing the minimum information necessary. This would undermine all of our efforts to assure that patients receive the right care at the right time at the right price. Simply put, providers need complete and timely access to patient information, and as pointed out in the recent report of the Institute of Medicine, access to complete information is necessary to prevent wrong care.

Third, we are concerned that the business associate provisions are unworkable, requiring business associates to establish procedures and notices consistent with the myriad of covered entities with whom they contract, and that would create an exponential numbers of different standards for business associates.

And fourth, our customers want practical rules that facilitate their interaction with their doctors and hospitals and health plans. We are concerned that the required consent provisions applied to providers will generate negative downstream effects on our customers as you have heard this morning. We are concerned about these real-life implications.

I want to spend a moment talking about cost. I want to be clear, for us the question is not whether privacy will increase costs, because it will. The issue is whether the regulation costs more than what it needs to, and we think it does. In addition, the high costs and other problems included in the privacy regulations are exacerbated by the HIPAA transaction and code sets that were released last August. These transactions regulate doctors and hospitals and health plans to reorganize their operations and codes and reengineer their systems in yet another way in less than 2 years. They are massively more complex and costly than Y2K, and many providers are unaware at this point of what they need to accomplish.

Anthem and the Blue Cross and Blue Shield Association support administrative simplification; however, we believe a 24-month implementation period is inadequate and should be extended. We believe that because we think the standardization of medical codes and the elimination of local codes is complex and very time-intensive. This requires not only major system upgrades, but is extremely resource-intensive. And these codes are intertwined

through every aspect and every function of providers as well as health plans.

Second, the staggered release dates of the various rules will make it difficult and costly to reengineer all the systems. In other words, we are effectively building the house before the blueprints have been signed off. Anthem and the Blue Cross and Blue Shield Association are advocating that the implementation time period for all the rules and administrative simplification be released in one final form. In other words we need those blueprints. This will allow health plans and providers adequate time to implement and test the new systems, spread costs and allow for proper provider education. Thank you.

[The prepared statement of Robert Heird follows:]

PREPARED STATEMENT OF ROBERT HEIRD, SENIOR VICE PRESIDENT, ANTHEM BLUE CROSS AND BLUE SHIELD ON BEHALF OF BLUE CROSS AND BLUE SHIELD ASSOCIATION

Mr. Chairman and Members of the House Energy and Commerce Subcommittee on Health, I am Robert Heird, Senior Vice President for Anthem Blue Cross and Blue Shield, testifying on behalf of the Blue Cross and Blue Shield Association (BCBSA). BCBSA represents 46 independent Blue Cross and Blue Shield Plans throughout the nation that provide health coverage to 79 million—or one in four—Americans. As part of the Blue Cross and Blue Shield system, Anthem Blue Cross and Blue Shield provides coverage to more than seven million members in eight states including: Connecticut, Maine, New Hampshire, Colorado, Indiana, Kentucky, Nevada, and Ohio.

We appreciate the invitation to testify today on the final privacy regulations issued by the Department of Health and Human Services (HHS) on December 28, 2000. This testimony provides us the opportunity to view these regulations through the eyes of our customers—and to identify and discuss those issues that will have the most significant impact on them.

BCBSA believes that safeguarding the privacy of medical records is of paramount importance. We support a basic set of clear federal rules for the health care industry that assures all consumers their health information is kept strictly confidential. At the same time, we know that our members demand and value superior customer service. Any set of rules needs not only to allow for timely delivery and payment of health care services, but also minimize hassles and costs.

During the comment period following promulgation of the proposed rule, BCBSA submitted over 50 pages of detailed comments and recommendations. It is clear from the final regulation that HHS took into consideration many of our comments and sought a balance in the final rule.

However, despite their efforts, the regulation still needs significant revision. Without substantial changes, the regulation is likely to slow the delivery and payment of care to consumers and the providers who take care of them.

There are significant new provisions in the final rule—some of these represent improvements, but many other areas require more thought and opportunity for comments.

Because of our existing concerns and the need for further analysis, we are pleased that the Department of Health and Human Services has provided another comment period to allow additional time to identify the many serious problems in the final regulation that would harm consumers. We are committed to helping HHS identify those problems and construct and implement a regulation that maximizes consumer protections, while preserving the ability of the health care system to provide efficient, quality services to consumers. We urge HHS to correct the serious problems in the regulation before asking the health care community to begin implementation.

In today's testimony, I will discuss two aspects of the Health Insurance Portability and Accountability Act (HIPAA). First I will focus on the final privacy regulation issued late last year. Second, I will discuss the closely related HIPAA Administrative Simplification Transactions and Code Set regulation issued last August. And finally, I will discuss the costs and savings associated with these regulations:

I. Privacy Regulation
   A. Background on Privacy
   B. Key Concerns with the Regulation
   C. Positive Aspects of the Regulation
   D. Recommendations on Privacy

I. PRIVACY REGULATION

A. Background

The Health Insurance Portability and Accountability Act (HIPAA) provided HHS the authority to promulgate privacy standards for health information if Congress did not pass legislation by August 1999. The statute was very narrow and directed HHS to issue privacy rules to assure that information transmitted as part of the new HIPAA standardized electronic transactions would be kept confidential.

The final regulation 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 (providers would be required to obtain consent even for treatment, payment, and health care operations);
- 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 associates to require them to use and disclose information according to the new privacy rules;
- Institute procedures to assure that only the "minimum necessary" information 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:* The privacy standards under HIPAA were intended to apply to electronic transactions that are developed and maintained under the law's Administrative Simplification provisions. While the proposed rule's application to paper records was arguably ambiguous, the final rule clearly applies not only to electronic records, but also to any individually identifiable information "transmitted or maintained in *any* other form or medium."
- *The Regulation Affects Internal Uses of Information as Well as Disclosures:* A common misconception regarding the regulation is that it regulates only the disclosure of information to a third party. In fact, the regulation has enormous implications for the *use* of information *internally within* an organization. This means that organizations will be required to comply with rules for internal treatment purposes, claims processing, utilization review and other routine health care purposes even though the information never leaves the organization's possession.
- *The Regulation Affects a Broad Array of Organizations and Information:* The definition of "covered entity" is broad in scope—including not only doctors, hospitals and health insurers, but also employer health plans (insured and self-funded, except for self-administered plans with fewer than 50 participants), laboratories, pharmacists and many others. All organizations that service health care organizations that are not included specifically as a "covered entity" are indirectly subjected to the privacy rule through a provision that requires covered entities to contract with their "business associates." For instance, lawyers, auditors, consultants, computer support personnel, accountants and other non-health oriented organizations would fall into this category.

  In addition, the definition of "protected health information" (PHI) is much broader than what most individuals consider their health information. The definition goes beyond an individual's medical records to include insurance records, oral information, and demographic data.

B. Key Concerns with the Privacy Regulation

Our overall concern with the final privacy regulation is that its intricate complexity will require a major reorganization of every doctor's office, hospital, pharmacy, laboratory, research facility, and health plan—as well as other organizations. We expect the final rule will lead to extremely costly infrastructure and procedural changes in each and every entity. For example, new sound-proof walls and offices may need to be built in health care facilities, new computer systems may need to be installed, and more lawyers and training personnel may need to be hired.

Although BCBSA has a number of concerns with the final rule, we have highlighted the four most problematic regulatory provisions in this testimony:

1. Dual Federal and State Regulation

The privacy regulation layers a new comprehensive set of federal rules on top of an already existing complex patchwork of state privacy laws. The regulation follows the HIPAA regulatory construct in that state laws are preempted only if they are contrary to the regulation and are less stringent. In addition, the regulation specifically "saves" certain state statutes from preemption, such as those relating to health surveillance.

We know our customers want a clear understanding of their privacy rights. However, we are concerned that the intersection between state and federal privacy laws under the complex construct of the HIPAA regulatory model will create more red tape and frustration for health care providers and consumers. It will be unclear whom to call for resolution on specific rules—HHS or the states— and this lack of clarity will lead to more telephone calls, more steps, and more hassles for everyone.

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 necessity for rapid transfer of information in today's health care industry because of the mobility of patients. 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 will have to 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 are likely to prepare conflicting interpretations—possibly leading to costly litigation with the states, the federal government and consumers.

This regulatory construct will be problematic for our customers. Instead of facilitating a member's ability to know his or her privacy rights, this complex preemption process is sure to confound that individual. First, individuals will be hard pressed to determine which aspects of the state and federal privacy laws apply to them, so it will be extremely challenging 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 gives up.

Our preference—and the clearest path for everyone in the system—would be for federal privacy law to preempt state law. Having a clear federal law would provide consumers and doctors with a clear path when answers are needed. However, we recognize that a complete preemption of state law is outside the statutory authority of HHS. Therefore, in our comments on the proposed rule, we recommended that HHS prepare a detailed privacy guide for each state explaining how existing state laws intersect with the new federal rules. We asked that the guide also address whether a privacy provision is triggered by a consumer's residence, location of provider or other criteria and that HHS prepare the guide in collaboration with state government officials. We also asked HHS to assure the guide incorporates other federal privacy laws, such as the Federal Privacy Act and Gramm-Leach-Bliley Act. As part of this process, we recommended that each individual state should certify agreement with HHS' analysis so everyone has a clear understanding of the rules.

We believe this legal guidebook needs to be prepared well in advance of implementing 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 consume a significant share of health care dollars. It is critical that these affected entities only have to modify systems and other items once.

Unfortunately, HHS failed to provide for this legal guide in the final regulation. In the preamble to the final regulation, HHS said that "many commenters" requested a similar state by state analysis. However, HHS declined to perform the analysis for the same reason they decided against a formal advisory opinion process: First of all, they indicated that "such an opinion would be advisory only . . . it would not bind the courts." In other words, they felt that even with HHS guidance, there was no guarantee regarding final decisions or outcomes.

Second, HHS indicated that workload issues drove their decision against formal preemption guidance. The preamble says that "the thousands of questions raised in the public comment about the interpretation, implications and consequences of all of the proposed regulatory provisions have led us to conclude that significant advice and technical assistance about all of the regulatory requirements will have to be provided on an ongoing basis . . . but we will be better able to prioritize our workload . . . if we do not provide for a formal advisory opinion process on preemption as proposed."

We urge HHS to reconsider this decision and issue a state-by-state analysis prior to implementation of the final rule.

2. Minimum Necessary Standard

The 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. At first blush, this standard seems to be a perfectly reasonable, common sense provision.

However, we are concerned about how we can best operationalize this concept without creating significant unintended consequences. 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."

This standard may require a massive reorganization of workflow as well as possible redesign of physical office space, and could jeopardize the quality and timeliness of patient care, benefit determinations and other critical elements of the health care system.

Many news accounts have inaccurately portrayed this provision as including an exemption for treatment purposes. HHS includes a very narrow exemption in the final rule—for "disclosures to or requests by a health care provider for treatment." This exemption does not cover "use" of the information, nor does it cover "disclosures by" providers. As a result, the minimum necessary rules may still place artificial limits on the ability of doctors to use and disclose health information for critical treatment situations—threatening the overall quality of care.

A few examples of other potential problems with the minimum necessary rule include:

- 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. Discouraging the sharing of complete medical records would make it more difficult to guard against these medical errors. 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 critical to use complete medical records for a variety of important quality assurance functions, such as accreditation and outcomes measurement.
- 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. For instance, the sign-in sheets used in doctors' offices are also used to verify that doctors are seeing the volume of patients they report for payment purposes. It does not appear that the privacy regulation would allow for these sign-in sheets to continue to be used.
- 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—a likely violation of HIPAA. Another example of potential renovation is an orthopedist's office, where the x-ray lightboard is centrally located outside of the patients' rooms for easy access by the physician. Anyone in the office could view these x-rays containing patient social security numbers or names. 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 privacy regulation. If implemented, this could impose incredible costs on consumers—not just in dollars and cents—but in lives as well.

3. Business Associates

The business associate provisions of the regulation require that doctors, health plans and other covered entities use prescribed contract terms with all of their "business associates" to assure these associates follow the HHS privacy rules. Doctors, health plans and other covered entities could be subject to civil monetary penalties if they "knew" of privacy violations by their business associates.

The contractual specifications included in the regulation compound the problems in the business associate framework. The rule requires business associates to use and disclose protected heath information in accordance with the notice and policies and procedures **established by the covered entity with whom they contract.** Many business associates will contract with multiple covered entities—each of whom have their own set of notices and their own uses of health information. This will create an exponential number of differing standards for business associates.

The confusion is exacerbated because some organizations—like health insurers—are covered entities in some areas (e.g. a healthcare coverage provider) and business associates at other times (e.g. third party administrator). Keeping track of what kind of relationship and what contractual rules to follow with which organization will be very difficult, confusing and time-consuming.

For example, Anthem Blue Cross and Blue Shield has many different relationships with other organizations. Anthem plays the role of licensed insurer and third party administrator (TPA) for medical and dental plans. Anthem is a pharmacy benefits manager (PBM) as well. In some cases, Anthem would be considered a covered entity; in other cases we would be considered a business partner. In fact, in some cases, like when we perform coordination of benefits (COB) with other insurers, both Anthem and the other insurer would be acting as covered entities, not as business associates of each other. We would not only have to follow rules as a covered entity but a host of other organization's rules and procedures as their business associate.

The timeframe for re-negotiation of contracts with business associates is also a significant problem. Health plans and other covered entities will have two years to update contracts in conformance with the privacy rule. Considering the multitude of relationships that we have with other organizations, we are concerned that two years is insufficient time to inventory all business associate relationships and renegotiate contracts. Moreover, if a contract lacks a unilateral agreement clause that allows the health plan to change the contract only with respect to the privacy rule's requirements, the entire contract could be opened up for re-negotiation—a time-consuming process possibly involving discussions over new payment rates and other contract clauses.

And finally, we believe the business associate 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. By attempting to indirectly regulate other organizations, we believe HHS acted beyond its regulatory authority.

4. Consent and Individual Restrictions

The final regulation requires health care providers to obtain consent before using or disclosing protected health information for treatment, payment or health care operations. In addition, it allows individuals to ask the provider to restrict the use or disclosure of certain health information.

We remain concerned that a requirement to obtain consent for treatment, payment and health care operations could unintentionally delay and impede routine operations that are essential to providing quality care and timely payment.

The regulation's transition rules allow providers to use and disclose information collected prior to the compliance date based on a patient's prior consent. However, if a provider has not obtained a new consent by the compliance date for treatment, payment or health care operations, he/she would be unable to use or disclose information collected after April 14, 2003 for that patient. The regulations anticipate that providers would simply obtain consents when patients arrived for treatment. The rule also states that consent forms obtained before the compliance date may meet the rule's requirements—however many providers may not have consents on record, and if they do they may not be for treatment, payment and health care operations—but only for one of these imperative functions.

Imagine that a mother is calling her pediatrician on the phone for advice on her sick baby. Her last actual visit was well before the compliance date and there is no consent on record. Does that mean the pediatrician cannot look at the child's

medical record while on the phone? What about an individual calling on behalf of an elderly relative for clarification about a particular medication but with no consent for that individual to access information? Or requesting additional payment information where the historical consent on file was only for treatment?

If a provider obtains a new consent but it does not list "payment" or "health care operations", there may be downstream impediments for some routine operations because providers could only disclose information for treatment purposes. For instance, claims may not be able to be paid, case management programs could suffer, and special pharmacy programs and other programs that benefit consumers also could be impaired because disclosures for these purposes depend on consent forms including treatment and health care operations.

C. Positive Aspects of the Privacy Regulation

Clearly, we believe there are significant issues in the final privacy regulation. However, HHS did address many comments in the final regulation in their effort to balance operational impacts with the overall goal of privacy.

A few of the most positive elements in the final regulation include:

- *"Statutory" Consent for Treatment, Payment and Health Care Operations for Health Plans:* The regulation does *not* require a new consent for treatment, payment, and health care operations for health plans. We believe a "statutory" consent, meaning that covered entities may use or disclose protected health information without consent as a matter of law, is imperative.

  Requiring health plans to obtain a new consent from current members 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 consents. In the interim, members and providers would experience delays in payment and other services.
- *Improved Definition of Health Care Operations:* The final regulation includes a modified definition of what constitutes "health care operations" that reflects many of the comments received by HHS. The definition is critical since items encompassed within it are exempt from new authorizations and tracking of disclosure requirements that would create obstacles to conducting essential health plan activities.

  We are pleased that HHS has incorporated many important and routine health plan activities into the final rule's definition. For example, we believe the definition may now allow health plans to continue many of their beneficial disease management and other quality improvement programs. The new "business management and general administrative activities" category will facilitate routine plan operations such as security activities, data processing and general maintenance. The "business planning and development" category will help plans to continue to develop more cost-efficient services and products.
- *No Third Party Liability in Business Partner Contracts:* The final rule deletes the requirement that makes individuals third party beneficiaries of business associate contracts. We support deletion of this clause since HHS did not have the authority to create a new private right of action. The third party liability clause was not only beyond the scope of HHS' authority, but it would have left health plans and other covered entities exposed to substantial liability for breaches of privacy by business associates.

D. Recommendations on the Privacy Regulation

While we continue to analyze this complicated rule, our specific recommendations to date are:

(1) Provide a Detailed Analysis on Preemption of State Law (A Road Map for Consumers): 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 compliance 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) Change the Minimum Necessary from Legal Standard to Guiding Principle: While we believe the minimum necessary standard is a laudable goal, we are concerned that it would be extremely difficult and expensive to implement this standard operationally and comply with it as a legal standard. Therefore, we recommend that HHS ask organizations to include the minimum necessary standard concept only as a guiding principle, not as a legal standard.

(3) Remove Business Associate Provisions. The business associate provisions should be removed from the regulation because they are:

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

At a minimum, we feel the business associate provisions should be changed as follows:

- Covered entities should not be considered business associates of each other; and
- Covered entities should be given at least three years to re-negotiate contracts and come into compliance with the business associate provisions.

(4) Provide a Statutory Consent for Health Care Providers: In the proposed rule, HHS recognized some of the operational problems of requiring authorization forms for treatment, payment and health care operations. We agreed with HHS' views, but recommended that covered entities be given the flexibility of requesting authorizations for treatment, payment and health care operations. The proposed rule would have actually prohibited it, unless required by State or other law.

We are pleased that the final rule retains a statutory consent for treatment, payment and health care operations for health plans, with the flexibility to request a consent if desired. However, we have concerns that the final rule *requires* health care providers to get consent for these essential functions. We feel that required consent may lead not only to operational issues, but could also affect treatment activities and quality of care.

(5) Include 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.

II. ADMINISTRATIVE SIMPLIFICATION AND THE TRANSACTIONS AND CODE SETS REGULATION

HHS' authority to promulgate privacy regulations specifically stems from Subtitle F of HIPAA—Administrative Simplification. Subtitle F was intended to facilitate the development of electronic data interchange (EDI) in the health care industry. In addition to the privacy regulations, this Subtitle directs HHS to establish national code sets, electronic standards for certain routine transactions, security rules, and standard identifiers for providers, health plans, employers and individuals.

In August 2000, HHS finalized the first of a series of regulations implementing the administrative simplification provisions of HIPAA. This first final rule standardizes electronic transactions used by health plans and providers for several routine functions (e.g., claims submission, eligibility inquiries, remittance), and codes for services and procedures used by hospitals, physicians, drug stores, and other providers. The rule generally requires compliance by October 2002.

Although Blue Cross and Blue Shield Plans and many others in the health care community have been working diligently to implement the transactions and code sets final rule, we have uncovered significant obstacles that make it unlikely that the health care community can complete implementation by 2002 without significant disruption and assumption of unnecessary costs. We urge HHS and the Congress to recognize the significant implementation problems that exist and to extend the implementation timeframe. Other organizations, such as the National Governors' Association and the American Medical Association also are calling for an extension.

We believe the current compressed implementation timeframe is inadequate and will lead to significant cost issues which we discuss in the next section of testimony. In addition, the current time frame will prevent resolution of numerous unintended consequences and the fact that there is limited availability of technology resources.

Unintended Consequences

The scope and complexity of the changes required by HIPAA will be difficult to implement during a two-year time frame, let alone test thoroughly. The two-year implementation timeframe simply does not allow time to test the massive system changes that are required. Without proper advance testing, system glitches will result in incorrect payments, complete payment breakdowns and other service problems that would hurt both consumers and doctors. The system breakdowns could also impede the answering of basic customer service questions, responding to provider eligibility inquiries, and other critical functions.

Even more importantly, with less than 19 months of implementation timeframe remaining, numerous key issues remain unresolved. For example:

- There are several new mandatory code sets that the industry has little or no experience using—such as the NDC drug codes. The implications of changing from J codes to NDC drug codes have not fully been realized or resolved to date—for instance, how will these changes affect payment policies?
- Standardized national code sets preclude the use of local codes for commercial use and this may have unidentified repercussions. The use of locally developed non-standard codes is particularly prevalent for home health services, long term care services and certain mental health services. Not only do the national code sets have to adopt new codes for these areas—a traditionally time-intensive process—but the new codes must be adopted and distributed in time for covered entities to make extensive system changes, train their personnel and evaluate any impact the new codes will have on payment, different state and federal laws, and other issues. To maximize efficiency and minimize costs—these codes should be available at a date prior to when providers and health plans begin their major system upgrades to implement the HIPAA standard transactions. At this point, it is questionable as to whether these codes will even be ready by the compliance date.

  In addition, today local codes are used to reimburse for new technologies, to respond to state legislative mandates and to comply with employer benefit administration requirements. It remains to be seen how these new codes will be developed and distributed in a timely basis after October 2002. A system to address new code adoption on an accelerated basis should be established—and tested for operationability—prior to HIPAA implementation.
- A preliminary comparison of the new claims transaction and paper claim formats have identified 60 differing data elements to date. These data elements are included in the electronic standard but are elements that providers do not currently have to collect, store, or transmit as part of the current process. In the future, all providers will need to be able to gather and input these new data elements. This will change the way all providers operate—including those that are paper-based only. The implications of these data changes need to be understood and communicated to covered entities before a successful HIPAA implementation can occur.

Limited Availability of Technology Resources

Hospitals, doctors, and health plans will be simultaneously revamping their systems to meet HIPAA compliance standards between now and October of 2002. This will generate an extraordinarily high demand for programmers, consultants, and other technical experts. Given the tight job market and shortage of technology professionals, it is unlikely that the technology community could meet this demand within the current implementation timeframe.

Additionally, vendor readiness and availability will directly impact the ability of hospitals, doctors, and payers to even begin to assess HIPAA needs. According to a recent Gartner Group Survey, 74 percent of healthcare organizations—payers and providers—expect to require assistance from consulting firms or systems integration firms to complete HIPAA assessment projects. Despite this great demand, only 15 percent of those surveyed had begun to assess HIPAA needs.

Finally, many providers and payers are dependent on vendor software to become compliant. Yet several major vendors have indicated that they will not have compliant applications available until the end of the first quarter of 2002. This further reduces the time the industry will have to implement and properly test systems. In addition, with less than 19 months left for implementation, Tillinghast-Towers-Perrin indicates that they are not aware of *any* provider clearinghouse or billing agency that is fully HIPAA compliant at this time.

III. THE COST OF THE PRIVACY AND TRANSACTION AND CODE SET REGULATIONS

As we discussed previously, BCBSA supports a basic set of privacy rules for the health care industry that assures consumers that their health information is kept private. We recognize that assuring consumer privacy involves additional resources. For us, the question is not whether privacy will generate costs, but whether the costs are more than they need to be. We believe a new final rule could be structured in a way to provide our customers with a better value.

HHS estimated the proposed privacy regulation to cost $3.8 billion over five years. HHS updated its cost estimate in the final rule to be almost $18 billion over ten years—more than double its estimate for the proposed rule. However, we believe HHS' cost estimates continue to be understated.

In response to the original proposed regulation, BCBSA commissioned Robert E. Nolan Management Consulting Company to provide an independent estimate of several key provisions of the proposed regulation. Nolan estimated more than $40 billion over five years in added costs for health plans, providers and other members of the health care community. A new, soon to be released, analysis by Nolan indicates most of these costs remain applicable to the final privacy regulation and that HHS continues to dramatically underestimate the potential costs of the privacy standards.

For instance, HHS assumes that the privacy officer function will be assigned to a current employee and only will add 15 minutes of time per week for non-hospital providers on an ongoing basis, and only 1.5 hours for hospitals and health plans per week on an ongoing basis. Nolan believes that the breadth and weight of responsibilities of a privacy officer will consume significantly more time and many organizations will assign a full-time officer. This is just one example of a privacy standard for which we believe the HHS estimates are low.

The final privacy regulation assumes that the privacy costs will be fully offset by savings from the implementation of the administrative simplification standards. We believe that the cost of administrative simplification implementation has been underestimated by HHS as well, and that smaller and rural providers will find it especially challenging to absorb these very significant costs. For instance:

- *Code Standardization Triggers Costly Process:* One of the most significant changes required by the transactions and code set August rule is the standardization of all codes. Providers will now have to use the exact same codes for every procedure, instead of a host of locally grown codes. This requires not only major systems upgrades, but is extremely resource intensive because codes are interwoven throughout every function a provider performs (e.g., treatment, quality assurance, fraud detection).

  Because of the August 2000 release date of this rule, many hospitals were unable to include these costs in their 2001 budget cycle and have not allocated funds. Smaller providers and rural providers will find it especially challenging to meet these cost requirements.
- *Staggered Rule Release Increases Costs:* It is important to recognize that the transaction and codes sets rule is one of several rules composing HIPAA. The industry expected that it could implement all the rules (i.e., security, privacy, transaction/code sets, and identifiers) as part of one comprehensive system upgrade. However, only privacy and the transactions rule are in final form. The staggered nature of the issuance of these rules will unnecessarily increase compliance costs by requiring covered entities to continually revisit system changes. Ultimately, these expenses will be passed onto consumers and employers through the increased cost of medical care.
- *Current Timeframe Creates Unnecessarily High Costs:* The 24 month timeframe (now fewer than 19 months) precludes covered entities from making HIPAA changes as part of the normal systems replacement, consolidation, and upgrade process. As a result, many organizations will have to waste valuable resources making older, existing systems compliant—even though those systems already are slated for replacement. Additional implementation time would allow the industry to spend resources more efficiently by converting to a new HIPAA compliant system from the outset—instead of upgrading and then eliminating old systems.
- *Timing Could Drive Providers Away from EDI:* Many providers will be unable to become HIPAA compliant within the implementation timeframe remaining. Some of these providers already submit claims electronically, but will revert to paper claims once the HIPAA deadline is reached. This would run counter to the goals of HIPAA, and would unnecessarily increase costs as well. Rural providers and those with limited resources will be the least likely to have the capacity to comply and thus realize the benefits of standardized EDI.

Because of our concerns regarding the cost impact of administrative simplification on providers, BCBSA asked Tillinghast-Towers-Perrin (TTP) to analyze the provider costs of the administrative simplification transactions and code sets rule released in August.

The TTP study predicts implementation costs significantly higher than those estimated by HHS: it estimates that hospitals will incur costs between $775,000 and $6 million for the transactions and code sets alone. HHS had estimated costs of $100,000 to $250,000.

The TTP report also indicates that physician's offices with 3 or fewer physicians are expected to incur between $3,000 and $10,000 of costs, while offices with upwards of 50 physicians could incur costs between $75,000 and $250,000. HHS had

estimated physician costs of $1500 for three or fewer physicians and $4,000 for groups of three or more.

In addition to estimating costs that were three to twenty-four times higher than HHS, TTP also reported that many hospitals may be underestimating the cost to migrating to standardized formats. A TTP survey of hospitals found that none of the survey respondents had completed comprehensive budgets to implement the electronic standards.

In addition, only a few hospitals had completed even preliminary ROI analyses and those few analyses do not account for ongoing changes to standardized formats once they are implemented. For example, it is highly likely that the American National Standards Institute (ANSI) will recommend movement to the International Standard Format in the near future that the remainder of the business world already is adopting. Consequently, three years from now it is likely that the health care industry will be implementing the international standard, souring any ROI projections that have been adopted today.

C. 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. We also look forward to working with you to adopt a workable timeframe for the implementation of administrative simplification transactions and code sets.

Mr. BILIRAKIS. All right. The bells again. There is a series of votes. It is more than one vote, so we are going to break long enough to give you an opportunity to grab a bite if you would like, and to give you some stability here in terms of a certain time. But I just wanted to give you something to think about during the break. I daresay there isn't a single one of you that does not want to do something from a privacy standpoint, and that something should be something substantial, that is real.

As I understand it, the implementation would be effective April 14, this year. But the compliance would not really take effect until 2 years hence. Does that mean that the providers and the patients, do not have to do anything for 2 years, or does that mean that the rule is in effect, and they have to follow the regulations during that period of time, however, they can't be punished until the compliance period is met? Is that correct? It is something that we want to find out. I see Ms. Goldman shaking her head.

I daresay probably at least half of you, if not all of you, know more about this than we do.

I guess my point goes to the fact that we want privacy, and we want it as soon as we can have it. Every one of you has indicated that you want the regulations; however, you would like to see some changes made to those regulations. You feel that there are some weaknesses in certain areas that have you mentioned in your testimony, and that there are other areas.

As I understand it, once the regulations go into effect, they can't be changed for 1 year, and any changes to those regulations, other than rate changes that directly affect compliance, or other areas that need to be cleared up, would have to go through the same process of comment period. So I think we are talking about quite a delay in any changes to these regulations if, in fact, they go into effect. Which they automatically would after the comment period is concerned.

The point is that we want this done right. We want it to be done as soon as possible. But I am not sure that we are going to get it done right if we have the regulations go into effect immediately

after the comment period, which is up at the end of this month. So we don't have much time.

We have 6 minutes, so we are going to have to run. Just think about it, Ms. Goldman. If you have responses or answers to it, which I trust you do. Thanks. So we are going to break until 12:45.

[Brief recess.]

Mr. BILIRAKIS. The hearing will come to order. Again, the Chair apologizes to the witnesses and to the audience, but this is commonplace up here, unfortunately.

I would, with unanimous consent, place into the record a letter dated March 13 from Helen Ellis Memorial Hospital, Tarpon Springs, Florida, to Secretary Thompson; and a letter dated March 16 from Eckerd Corporation to me.

Without objection, those will be made a part of the record.

[The letters referred to follow:]

HELEN ELLIS MEMORIAL HOSPITAL
March 13, 2001

TOMMY THOMPSON, *Secretary*
U.S. Department of Health and Human Services
Attn: Privacy I, Room 801
Hubert H. Humphrey Building
200 Independence Avenue, S.W.
Washington, D.C. 20201

RE: Standards for Privacy of Individually Identifiable Health Information

DEAR SECRETARY THOMPSON: On behalf of Helen Ellis Memorial Hospital in Tarpon Springs, Florida, I am writing to comment on the Department of Health and Human Services' final rule implementing the medical Privacy standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Helen Ellis, and all hospitals, are committed to Protecting the Privacy of their patients' information. We believe that patients have the right to every consideration of Privacy, including the right to review and understand medical records. However, in their current form, the rules are so complex and prescriptive that they are both unworkable and excessively costly.

Therefore, we strongly urge HHS to suspend the April 14, 2001 effective date and to fix the rules and get them right. *Hospitals should not be asked to begin implementing a rule that needs to be fixed.*

We have many concerns about the final rule. Here are the most pressing:

- **Consent** (§ 164.506)—Reform the rule and grant hospitals sole discretion to determine whether and how to obtain consent from patients for information used or disclosed for purposes of payment, treatment and health care operations.
- **Minimum Necessary** (§ 164.514)—Reform the rule and eliminate applicability of minimum necessary requirements—the single most costly requirement under the rules to uses of information for treatment, and substantially revise them for other uses.
- **Oral communications** (§ 164.501)—Reform the rule and eliminate its applicability to oral communications. HHS clearly exceeded its statutory authority in extending the rule's prohibitions to oral communications and, unless reformed, this requirement could stifle doctor-patient communications.
- **Business Associates** (§ 164.502)—Reform the rule, including eliminating restrictions that would prevent third parties from sharing medical information among hospitals organizations that provided the information in the first place—for important quality improvement and assurance purposes.
- **Implementation Date** (§ 164.534)—Reform the rule and delay the implementation date to a workable, more realistic time frame beyond the current two years.

By suspending the rules and fixing them according to these recommendations, the result will be an improved, more effective privacy regulation.

Thank you for considering this request.

Sincerely,

JOSEPH N . KIEFER, FACHE
President/CEO

cc: U.S. Congressman Michael Bilirakis
U.S. Senator Bob Graham

U.S. Senator Bill Nelson

ECKERD CORPORATION
March 16, 2001

The Honorable MICHAEL BILIRAKIS
U.S. House of Representatives
Washington, D.C. 20510

DEAR REPRESENTATIVE BILIRAKIS: I am writing to request your help with revising certain portions of the recent federal regulations relating to medical records privacy. As currently written, these regulations would have an enormously negative impact on community pharmacy operations, threatening the convenience and quality of care that consumers have come to rely upon from their local pharmacists.

While we support strong protections for patient medical records, certain parts of the rule are simply unworkable and impractical. Specifically, *the final regulation requires a patient to provide a signed, written consent to the pharmacy before they can obtain prescriptions and other health care services.*

What this means is that a pharmacist could not recommend over-the-counter products and treatment without written patient consent. A parent with a sick child could not pick up prescriptions phoned in by a physician until a written consent is provided. Prescription refills called in after the regulation's compliance date could not be filled and ready for pick up until a consent is on file at the pharmacy. Moreover, after the compliance date, a pharmacy could not even remind patients to refill their prescriptions for chronic use medications.

Given that pharmacies expect to provide over 4 billion prescriptions in 2004 it is clear that these regulations would disrupt the lives of thousands of patients. The additional burdens, time, and cost imposed on patients and pharmacies by requiring this signed written consent far outweigh any additional privacy protections that would result from this approach.

Therefore, I am asking you to write Health and Human Services Secretary Tommy Thompson to urge him to remove the requirement that pharmacies obtain prior written consent from patients before they may use patient information for treatment, payment or health care operations. *Please write Secretary Thompson with this request by March 30, 2001, the deadline for public comments on this regulations.*

Please respond as soon as possible, so I may inform my colleagues of your actions on behalf of the community pharmacy industry. Thank you for your assistance.

Sincerely,

JIMMY JACKSON, R.PH.
Vice President Pharmacy Relations
Eckerd Corporation

Mr. BILIRAKIS. I have many questions for Mr. Ortiz, Dr. Clough, and Ms. Goldman; and we can go on and on regarding specifics, the effect on the neighborhood pharmacists for instance, on the current regulation and things of that nature. I also have a question for Dr. Appelbaum. I expect that we will have more members coming in as we talk here, and other questions will probably be raised. We will also ask that you respond to us in writing to questions that we will send to you in writing after the hearing.

But what I asked is kind of the bottom-line, and that is, do we put these regulations is to effect immediately, knowing that there are refinements that must be made? When could those refinements be made part of the regulations if we put these into effect at this point in time? It is my understanding that depending on the interpretation of what the refinement is, whether it is just a technical change, or whether it is a policy change will determine that.

So having gone into that and asked you all to think about it during the break, Dr. Clough, we can start with you, and hopefully you all can get your viewpoints in during my short period of time.

Mr. CLOUGH. We recommended delay. And although we agree with the importance of getting some regulations in place and making sure that people feel comfortable about privacy, we think that

there is a downside, a serious downside, to beginning to implement something which is wrong. And I would say that at our place if these—if this regulation does go into effect, we will immediately start spending money to make sure that we can meet them as they stand at that date.

It is sort of analogous in some ways to the Y2K issue. When the time approaches, you had better be ready. And you have spent the time and money to get ready. That cost us a lot of money, and I think it cost everybody a lot of money; and to some extent the outcome was ho-hum. But I think it was ho-hum because that money was——

Mr. BILIRAKIS. You are saying that if these changes can be made now before they become a part of the law, then fine. But if they can't be, you would want to see delays until they are done right.

Mr. CLOUGH. Not indefinitely, but for some period of time.

Mr. BILIRAKIS. Ms. Foley.

Ms. FOLEY. Our association would support that the regulations commence on the time that they have been identified to commence. And certainly if there are areas of interpretation for the Secretary for clarification because of some of the misunderstanding or interpretations, that would be very appropriate. But we think—in the public advocacy role, we support the sooner the better.

Mr. BILIRAKIS. But how about some of these areas that these good people have brought up, which are certainly beyond the realm of interpretation or clarification?

Ms. FOLEY. They are not my area of great expertise. I would be sensitive to them if they were barriers of the regulation. I think the regulation is well intended. Clarification is required.

Mr. BILIRAKIS. Comments were made previously by many members of this subcommittee that the Congress did not do the job, that we asked the administration to do it. They spent time doing so, and we appreciate that. You are right about that. It is just that some of these real practical matters are not included.

I am going to take the prerogative and say we have 10 minutes since my time is already up. Each one of us will have 10 minutes and no second round.

Continue on, Dr. Melski.

Mr. MELSKI. Yeah, the main issue is one of planning. When we fund large information systems projects out of our own budget, it often takes 3 to 5 years to implement them. You can always accelerate these timetables by spending more money and doing it more quickly, but to have uncertainty over a long period of time about exactly what is going to be changed creates havoc for us. Two-and-a-half percent of our revenue in your operations is to support clinic information systems in fiscal year 2001. That is $22,000 per each of our 600 physicians.

We are in capital equipment planning right now for the next fiscal year, which for us starts in October; and if we do not know how to plan, we have a lot of problems.

Our estimate of the direct personnel costs for getting consent from the 350,000 unique patients that we see each year—we can't wait until the final date. We have to start tooling up now, because if it took a half-hour to explain the notification in order to get valid consent, that is 175,000 hours; and it would take 103 full-time em-

ployees at 1,700 hours each, and $25,000 per employee or $2,575,000.

Now, you can't say, well, start planning, do your capital budgets, do your operational budgets, and then maybe in a year all the things that you plan for now are pulled out. What that does is, it hurts health care. In other words, we have projects that we are scrambling to do to decrease errors in medications, for example, we will have to put them at a lower priority so we can be in compliance with these applications.

Mr. BILIRAKIS. Doctor, forgive me. I want to get through.

Dr. Appelbaum.

Mr. APPELBAUM. Mr. Chairman, we understand these regulations will not go into effect, that is, compliance will not be required for 2 years after their formal adoption. We also understand that the Secretary has the authority within the first 12 months after formalization of the regulations to make whatever changes may be necessary.

Mr. BILIRAKIS. After the first 12 months, as I understand it.

Mr. APPELBAUM. During the first 12 months.

The Secretary—I have the language in front of me, Mr. Chairman, in section 160.

Mr. BILIRAKIS. Only to affect compliance, staff tells me.

Mr. APPELBAUM. Necessary to permit compliance with the standard or implementation specifications. And I think we would interpret some of the comments that were made here today as falling well within that standard. For example, no one ever intended these regulations to interfere with the ability of a family member to pick up a prescription at the neighborhood pharmacy, and clarification of that by the Secretary would be well within his authority under this standard.

Mr. BILIRAKIS. I know Ms. Goldman agrees with that. But she will speak for herself.

Mr. Ortiz.

Mr. ORTIZ. We believe they should be delayed. We are not sure that they can be fixed unless you go out with a new proposed rule. For example, the concept of statutory authorization which was in the original proposed rule and was deleted in the final rule, which would have allowed the pharmacies to accept the prescription as an implied consent to fill out that prescription is something that should be put back into the final rule. And I don't know that that can be done with simply delaying.

Additionally there are other components of this which we are waiting for before you can even begin to implement some of the necessary changes. For example, the security regulations are not finalized. I don't know how we can move forward in doing some of the software changes, et cetera.

Mr. BILIRAKIS. I don't want to get into details, Mr. Ortiz, because of time element, but thank you for that.

Ms. Goldman.

Ms. GOLDMAN. Mr. Chairman, I think there are two areas here, and if we could divide them up, this might make the conversation a little easier.

There are a number of policy differences that have been identified on this panel today, disagreements over whether there should

be a consent requirement or not a consent requirement. Those things—I think if the Secretary is going to make changes in those, he can probably make changes in those before the effective date.

Mr. BILIRAKIS. Before the end of the month?

Ms. GOLDMAN. Or before the April 14 date.

We do not support doing that. I don't want to signal that we do support doing that, but he certainly could do that.

The second area is the area where there are things that were not intended—as the title of this hearing suggests, things that were not intended by the legislation, glitches that might be in there, clarifications that are needed, guidance that the administration can issue or modifications, where necessary, to permit compliance as Dr. Appelbaum just cited, within the first 12 months of the regulation being effective. But that authority, the legal authority the Secretary would have to make those modifications, is not triggered until that April 14 effective date. Then within those first 12 months he could make those changes and we would support him doing that, so people do have the certainty they need to move forward.

Mr. BILIRAKIS. Thank you.

Mr. Heird.

Mr. HEIRD. April 14 is a shotgun start and we have 24 months to begin. If the rules change, as was pointed out by a couple of answers a moment ago, how much of that work is going to be thrown away while we restart? So that is a very serious concern of ours.

Also it seems that for the last 30 days the industry, all parties, are giving the Secretary comments. I don't understand how they could go through the comments they are going to receive in less than 2 weeks, make changes, and understand the impact of change A to change B to change C. So I think it is almost disingenuous not to think about change.

Mr. BILIRAKIS. I believe they have already received many of these comments. Some maybe they haven't.

Mr. HEIRD. But that is problematic.

Mr. BILIRAKIS. My time has expired.

Mr. Stupak, may I yield to the full committee chairman? Is it all right with you?

Chairman TAUZIN. Either way.

Mr. STUPAK. Thank you.

Dr. Melski, I am looking at your testimony and I see your cost estimate for the new rule. Could you describe the details that are assumed in your calculations that it is going to take 30 additional minutes for each patient? In all seriousness, I don't think there is anyone on this panel that has ever spent 30 minutes with the doctor, now you are telling us that you are going to spend 30 minutes explaining an informed consent.

Mr. MELSKI. You haven't met my mother.

Mr. STUPAK. Is she a physician?

Mr. MELSKI. No, but she is an example of an elderly patient who would be frightened by signing something she doesn't understand.

And you also have to understand that we are talking about children who are transitioning into adult life, where there are ambiguities about whose consent you actually need and the whole concept

of an emancipated minor and whether we get consent from them or their parents.

All of this has to be worked out. Not only does it have to be worked out, we have to track it.

Mr. STUPAK. Don't you really—in all seriousness, if you are going to do the mother or young child, don't you perform complicated procedures on them and don't you have to explain to them the complicated procedures that are going to follow? How can that be more complicated than explaining an informed consent?

Mr. MELSKI. I don't think it is, but why do you want to double the work?

Mr. STUPAK. If it doesn't take 30 minutes to explain a complicated medical procedure, why would it take 30 minutes to explain an informed consent? I think most people have an idea about privacy, and they do not want their name and personal information used outside of our procedure.

Mr. MELSKI. Your point is very well taken and so well taken that I am concerned, in practice, what will happen if people don't understand the notification. They will be coerced into signing; and I think that is a bad thing to do; I think people should not sign something they don't understand.

Mr. STUPAK. Before you do a medical procedure, let's say outpatient surgery, the patients sign a form allowing you to do that.

Have you ever asked any of your patients after they did that, did they understand what they just signed?

Mr. MELSKI. I understand very well the exact dilemma that you were talking about, and that is exactly why I am concerned about complicating it by adding another process that has the same problems of what is consent, what does it mean, and what value does it add? That is the real issue.

We have much common ground here. We really want to take care of people. We want to do the right thing. And I know it is dramatic to make it a good guy-bad guy kind of scenario, but we are all trying to do the right thing. But I genuinely believe that adding a consent with whatever time it takes, or if it takes very little time or it is meaningless because people are not really looking at it—see, I think the emphasis should be on the public disclosure. People should know what your privacy policies are.

We hope at Marshfield Clinic to set an example that other clinics in the Nation can follow. We have many of these things—we have been doing this for a long time. And we have very strong language to protect patients.

Mr. STUPAK. If you have been doing it for such a long time, how then does the Secretary's proposed rule differ from what you have been doing for a long time? Why should this be more complicated, that it is going to cost you over $2.5 million a year in direct cost?

Mr. MELSKI. The problem is that there are all kinds of costs that are not there. So if it is not a half-hour, it is 15 minutes.

Mr. STUPAK. I am basing it on your half-hour, 103 full-time employees, $25,000 per employee, that is 2.575 in direct personnel cost, to gather consents in the first year.

Realistically, look, you go in there, here is the operation, here is the consent. You will see maybe an anesthesiologist. I never see them the morning they put you under, but you sign for them. You

don't know who it is. The doctor may say I am going to use the Green Bay Anesthesiologists, and you sign for that. And here is your outpatient and here. Sign here so we can bill your insurance company.

I don't know one patient that sits there and reads it and then is quizzed by the doctor afterwards about what went on there.

Realistically you can give the forms to the folks, there is the privacy. The people understand it. It can't be more complicated to the people that understand it.

I take exception to 30 minutes, 103 full-time employees at the Marshfield Clinic.

Mr. MELSKI. Well, the average consents that we have for complicated surgical procedures are seldom more than a page or two. These notifications that were sent out as a model are nine pages long, single-spaced.

Mr. STUPAK. So if you can do a very complicated procedure that is only a page long, you are telling me that you can't do a consent that is a page long.

Mr. MELSKI. No, the consent is different than the notification. But the consent is required to refer to the notification, and unless people understand the notification, it is sort of like saying, sign here, but you have to go somewhere else to understand what you really signed.

That seems to me that that is not the kind of, it is just——

Mr. STUPAK. If they sign your consent form, why do they have to go somewhere else to understand it?

Mr. MELSKI. Because what they signed is saying you agree to something that is nine pages long, single-spaced;that is what they are signing.

Mr. STUPAK. You are saying that people are not smart enough to figure out the nine pages?

Mr. MELSKI. I think people are sick and they are sometimes ill and they are young and they are old and they have a lot of other problems; and so, yes, I am concerned that they don't know what they are signing.

Mr. STUPAK. Does anyone else share the concern that they do not know what they are signing?

Ms. Foley—Goldman.

Ms. GOLDMAN. Can I just clarify something that Dr. Melski said?

This nine-page notice that has been referred to a few times was not a notice that was put out by the administration. It is a notice developed by the American Hospital Association as kind of a worst-case scenario of what a notice might look like. As we saw—under the Financial Modernization Act, the notice that is required under there; I just got one in the mail the other day—it is a small brochure.

The notice that is required under the regulation could be a one-page notice; it does not have to be nine, single-spaced, complicated, overwhelming. And the notice is a notice about the regulation, not about the consent. It is about your rights under the regulation, what you can do about your rights to get access to your own medical records.

Their consent is not even a meaningful consent under the regulation. Yes, it is required, as consents are now required in health

care generally today, but it is a consent that could be coerced. You can say, you must sign this—and it could be one paragraph—you must sign this in order to get care in this facility, you must sign this in order for us to get reimbursement for your care. And the notice that is to accompany that is a much broader—serves a lot of different purposes, and doesn't have to look like one the AHA wrote.

Mr. MELSKI. I must say I am astonished by the phrase that the consent is not meaningful. I just heard you say you could have a consent that is not meaningful. How do we interpret that? How do we plan for that? What are you telling us?

Ms. GOLDMAN. Maybe what would be helpful is for you to try to explain what people currently do sign when they are admitted.

Most people do sign—when I say it is not meaningful, they can't say, we don't want to sign something that allows you to use my information to treat me, yet you must still treat me. In that sense, from a strict privacy standpoint, it is not meaningful because it is not voluntary. And it is not—it is meaningful in the sense that there is their signature, and they say they have signed it and they authorize the information to be shared. But they cannot withhold that authorization under this regulation and continue to get care and continue to get payment if that facility chooses not to do that.

Mr. MELSKI. The other area that complicates this is that there is preamble language that says, we could say that these consents are not revokable; but there is also strong language that says we should not do that. We are trying to do the right thing.

If we have a consent that is not revokable, this creates an administrative catastrophe because then we have to segregate records based upon whether the consent has been revoked or not; or once again, we have to exercise the prerogative that we were told we should not do, that they hope we will not, and that is put into our consents that it is nonrevokable.

Mr. STUPAK. People revoke their services all the time. They pay their bill and they leave. Because I revoke my consent and I no longer want you using my information, should I not have that right?

Mr. MELSKI. Let's get away from money. Let's take a child who has a broken arm by parental abuse and has it taken care of and revokes the consent for that to be revealed. You need to understand in child abuse it is the pattern of injuries over time that determines whether you have concern or not; and the parent could use the revoking of consent to hide from one provider to another a pattern of behavior.

Mr. STUPAK. But now we are talking about a criminal case, and in any child abuse case in any State, you as a physician have a right and a legal obligation to report it to the authorities.

Mr. MELSKI. This is absolutely true. That is certainly true in Wisconsin. That is a very good point.

I am trying to explain that my level of suspicion is based on a pattern, and the only way I can understand the pattern is to have access to the information of the care that was given previously. So when the consent is revoked, I have great difficulty doing that.

Not only that, we have questions about how we can process bills, what we have to do with the record, how we have to extract it or

segregate it electronically. The revocation sounds easy. It sounds superficial. But come talk with my programmers when we try and implement this.

This has profound implications, because you have to track this very complex situation of whether the consent is in effect or not; or what you have to do is, as suggested, make a consent that is nonrevokable, again adding to the intimidation factor. When you say, here, sign this, you can't revoke it and you are sick and you need help, what does that do to the trust relationship? How does that help.

Mr. BILIRAKIS. The gentleman's time, the 10 minutes, has long expired. I would appreciate it.

Mr. STUPAK. Thank you, Mr. Chairman.

Mr. BILIRAKIS. The Chair yields to the chairman of the full committee.

Chairman TAUZIN. Thank you, Mr. Chairman, thank you for this hearing.

In the opening statement I know was made a part of the record already, I quoted the Hippocratic Oath section, that says, "Whatever in connection with my professional service or not in connection with it I see or hear in the life of men which ought not to be spoken of abroad I will not divulge as reckoning that all such should be kept secret." That is the current oath that doctors, physicians, and health care providers take.

Mr. Appelbaum, I am holding in my hand a letter from the APA to the Secretary of Health and Human Services, I want to quote from it. It says that, and I quote, "Patients will lose some existing privacy protections because the current practice of hospitals, doctors generally requiring patient consent, notice of full disclosure, will change as a result of the regulation. Patients' ability to decide when their medical information will be disclosed outside the health system will be reduced."

The letter goes on to cite one of those cases. It points out that under this regulation "that attorneys can simply certify that the information requested concerns a litigant to the proceeding and the health condition of such litigant is at issue between," and the letter goes on to say, "These procedures provide no check on the attorney's behavior in requesting records of marginal relevance to a case or for the purpose of embarrassing and intimidating opposing parties."

That is a pretty strong statement. These regulations allow attorneys—in fact, require doctors to breach the Hippocratic Oath, and to give a patient's personal medical information to be used simply to embarrass without the court ever supervising the demand for this information.

You go on in your statement to cite seven other cases where you find these regulations significantly deficient. On the first of these, you are concerned that the language is not broad enough to protect all forms of psychotherapy, and that these requirements require a second set of records which most psychiatrists will not do. This will increase time, difficulty and costs associated with recordkeeping.

Third, you make the point that police officers, under these regulations, have the right, and I quote, "to simply issue written demands to doctors, hospitals, and insurance companies to obtain pa-

tient records without meeting with a judge to review the assertions."

You cite a further exception that allows the release of medical record information anytime the police want to identify a suspect. That is pretty broad loophole.

You mention that, additionally, administrative subpoenas or summonses are particularly troublesome because they do not have any judicial review, and doctors are consistently, under these regulations, required to compromise their oath and to turn over information to police, to lawyers, to administrative summons.

You mention on the next page the overly broad physician liability, because a physician is liable with his business partners, and the physician may have to keep track of his business partners to make sure that none of them violate the guarantee he's made to a patient. And you question, for example, whether this overly broad liability is going to create lawsuits against physicians for what business partners may do.

On the next page, you talk about the intelligence agencies and the State Department compromising private information under these regulations. You are particularly concerned about the requirement for broad access without a patient consent for disclosure of medical records of Foreign Service personnel and their families.

You go on to talk about the fact that the APA believes that the cost associated with these regulations is significantly understated; that a psychiatrist will experience significantly higher costs and will have heavy administrative burdens following this extensive and broad regulation.

And finally you ask, can a psychiatrist who does not have any staff and therefore is the privacy official, and if the privacy official makes a mistake, is he the only one liable or is the doctor liable too?

You ask some pretty significant questions in your statement. I read your statement in the letter from your association to the department, and you have got massive concerns about these regulations that need to get addressed, yet you tell us today we should proceed with this.

Can you reconcile what appears to be a very apparent conflict in those two statements?

Mr. APPELBAUM. I would be very happy to try to do that for you, Congressman.

These regulations give us what is clearly half a loaf. There are many ways in which they were inadequate, and you have cited many of them here this afternoon. And we could focus on those inadequacies and should at some point in an effort to correct them.

But there is the half a loaf that they do give us. They give us the first national standards for medical record privacy that provide some set of protections for patients which do not exist at the moment. They give us a requirement that entire pieces of medical records not be released when you can do with less. They give us protection for psychotherapy notes which may be the most sensitive information in those records. They give us the right to inspect and copy one's own health information and correct it if it is erroneous.

Chairman TAUZIN. They give you those protections unless a lawyer demands them.

Mr. APPELBAUM. They give you those protections unless many of the circumstances you cited occur.

Chairman TAUZIN. These regulations are desperately in need of repair. You are right. It is a good step. It is the right thing to do, to try to create medical privacy rights.

But you pointed out a list of real dangerous problems, and your association actually makes a case for these reduced patient rights, rather than expand them, when it comes to some people's right to access private information, but a doctor swears an oath he won't give it to anybody.

Mr. APPELBAUM. And in many respects they do, but we live in the real world.

Chairman TAUZIN. The real world is the Secretary is reviewing them now. He is taking public comment. He will be before this committee, we expect, next month. We have his commitment to do that, to tell us what he thinks about it.

But the real world is, we have a review process on. We have time to correct them and make them right. Don't you think we should do that?

Mr. APPELBAUM. I think we should correct them as best we can.

Chairman TAUZIN. Let me turn to the pharmacy issue, because it is a huge one.

Gentlemen, imagine—Mr. Chairman, I can't imagine going home to town hall meetings to face a public that tells me they can't get their prescription filled, that they have to sign these consent forms after they have already authorized their doctor to issue the prescription for them; and they send a wife or child or friend to go to the pharmacy to pick it up, and they come back empty.

I cannot imagine the first liability suit that will be filed because, as recently happened with one of my friends, he forgot his nitroglycerine and had to get some real quick and he shows up at a pharmacy—and I go to get it for him, and I can't bring it back for him, and something happens in the interim—you know, bad.

You make an awfully good case, Mr. Ortiz, that the patients have given their consent for the prescriptions. They go see the doctor. The doctor says I am writing out a prescription; go pick it up at the pharmacy. You have a problem. You can tell the doctor, I don't want you to have the pharmacy know I have this problem. I don't want that issued from that pharmacy. You can do it right there if you like.

But the fact that you make no objection, the doctor says, I have issued a prescription; here is a copy; take it to the pharmacy. And you take it in your hand and you give it to your niece, your uncle, or your friend or wife to go pick it up, and they come back empty-handed because the government issued a regulation that will not let them pick up your prescription for you. I can't imagine going to a town hall meeting and facing the complaints of my constituents on that.

I live in a rural area. There are not drug stores on every corner in the bayou, I promise you. And going to the drug store can be a difficult task for some people who are sick and infirm. They have to send somebody else to do the job for them.

And it occurs to me, Mr. Chairman, that when regulations are written without common sense like this, they really cause me to

step back and say, wait a minute. We had better examine every line, dot every I, cross every T that has to be crossed in these regulations before I have to go home and answer to constituents that can't understand why we have done this to them when it was not necessary to protect their privacy.

Ms. GOLDMAN. Mr. Chairman, would you allow me to respond to that?

I could not agree with you more. I don't think there should be anything in these regulations that keeps a relative from picking up someone's prescription or keeps a pharmacy from being able to fill a prescription; and I actually do not believe there is anything in these regulations that prevents either of those activities.

And if there is a concern about whether or not next of kin, as it is clearly defined in the regulations, should be able to pick up a prescription, if someone has not acted affirmatively——

Chairman TAUZIN. Can you imagine us writing a rule defining which next of kin qualifies and which does not?

Ms. GOLDMAN. Excuse me, Mr. Chairman.

What I was trying to say is that in the regulation next of kin are able to receive information about individuals. Only if someone takes an affirmative step to limit a disclosure to next of kin will that occur. I cannot imagine that a pharmacist will not allow a relative or family member or even a friend to pick up a prescription, unless that individual said——

Chairman TAUZIN. Staff tells me that you are wrong, that is only true if they are under care, not if you are just picking up a prescription.

Mr. Ortiz is testifying to that effect.

Mr. Ortiz?

Mr. ORTIZ. First of all, in the preamble, which is not part of the——

Mr. BILIRAKIS. Let's keep it brief.

Mr. ORTIZ. In the preamble it says that the next of kin could possibly pick it up. That is only if, in fact, there is a filled prescription waiting for them to pick up. I am saying there won't be a filled prescription waiting for that individual to pick up unless we have that written, prior consent.

Chairman TAUZIN. I think we have it on the record.

Mr. Chairman, thank you. I want to say finally, we will have the Secretary here. I will assure the committee he committed to come and to brief us on what they are finding out.

I want to thank you for having this hearing, for giving us a chance to shed some light on it, because frankly I hope he does a good job of reviewing this regulation before it becomes final, and we fix it so that it isn't half a loaf. It is a good, full loaf and it is simple and it makes sense and it is practical. And when I go home to a town hall meeting, I am not roasted alive because I let this happen in a way that doesn't make sense.

Mr. BILIRAKIS. Thank you, Mr. Chairman.

Ms. Capps.

Mrs. CAPPS. Thank you. I would like to express my thanks to this large panel for your persistence and endurance through this testimony. It is really valuable to us; and I appreciate it and I hope Mr. Chairman you will allow me to confess that after Ms. Foley gave

her statement, I uttered a "Right on" to myself; I didn't say it out loud. Because I do appreciate the voice of nurses being heard on many of our health issues.

And I am thinking about this particularly with respect to the topic at hand. There are 2.2 million nurses across this country, and I daresay in the real world of today, where privacy is being both invaded and protected, as we speak, in a variety of health care settings that many of those consent forms are actually being corrected by nurses. And I want to give you a chance to talk about that. You are one of the most enthusiastic or optimistic about where we are right now.

In this country, I would imagine we have a patchwork of privacy protections, and again, nurses are experiencing all of this in various settings. And yet you remain optimistic that this is something we can go forward with, given the circumstances with which it was reviewed.

Can you summarize or describe the time and effort that you believe compliance with this regulation—what that will mean for providers of health care?

Ms. FOLEY. Thank you, Congresswoman. I appreciate the opportunity to explain a little further why we are optimistic.

While—on balance, many providers in this country are making their very best effort to meet this very standard; however, it is not uniform, and that is one of the reasons we were very supportive of it as a Federal regulation. In reality—and I appreciate the doctors' concern about informed consent, but in the normal course of nursing work, we are constantly informing and obtaining consent and verifying that the information is well understood and then thoroughly documented. That is very much a part of our role in the admitting and even in outpatient settings, all the way through each procedure and each test; and it is an ongoing process. And if it is time-consuming, it is time very well spent, so that people in our country understand the care they are receiving. And if the disclosure of information is part of that information that is shared, then well it should be.

So we really continue to support the principle that this is the right way to approach the information and that it is doable within the context of the many other commitments that we have.

I want to give an example, if I could, under the definition of the minimum necessary standards.

Mrs. CAPPS. Yes. I was going to ask you about that very thing.

Ms. FOLEY. I think that is an opportunity to give some of our real-world experience.

In balance of the treatment and in reading the clarification of the regulations and the provision, coordination and management of care, certainly the judgment prevails that in exchanging information that is appropriate, that is required to give full treatment. Let me give a quick example of two reasons, two ways we can look at this, and these are policies that already exist—at least in acute care settings that I am familiar with.

If I am the nurse and I have been asked to administer a unit of blood to a patient who needs blood, and I have a physician order to do so, and I have obtained the laboratory consent, the blood consent form from the patient, after informing them, verifying that

they understand the physician's information that they need to receive a unit of blood—and again this is with somebody who is competent, and I understand the doctor identified the issues for guardianship and competency—I will take this chart—in order to provide better patient safety, I actually take the full chart down to the laboratory.

And I, in my facility, was required to share with the laboratory technician the patient identification, the physician order and the blood consent form; and nothing else in that chart was to be shared with that lab technician nor would it have been appropriate for me to start flipping through the medication records, the surgical report or any other information. In other words, that minimum necessary for me to get a safe unit of blood for that patient specifically was indeed the standard, and it is common practice.

The dietitian wants information about the patient—minimum necessary could be more expansive. For example, they want to know what medications the person is on because of drugs, medication, adverse events.

I think the standard is quite interpretable, and in many cases, already well enforced by policy and practice in many of our institutions. And as employees of facilities—all of the employees, whatever category, licensed and unlicensed—are required to respect those policies and adhere to those confidentiality matters.

And so, again, it is a standard that most people strive for. The uniformity of a Federal regulation can only help us do better.

Mr. MELSKI. May I respond?

Mrs. CAPPS. Yes.

Mr. MELSKI. I agree. We basically—we have so much common ground here. That is why it is painful to cast it as a struggle. But what you just heard was a description of a person with a single role. We have a very complex organization where roles are constantly changing.

Mrs. CAPPS. Could I interrupt just for a second?

I believe the illustration was meant to lift out a single role in a very complex setting of health care.

Mr. MELSKI. Right. That is exactly my point.

That is, when we have nurses that need to cross-cover or change their roles from day to day, when we have to build electronic systems which track what role they are playing today and, therefore, the minimum necessary in their role this day is different than the minimum necessary in their role another day, this becomes exceedingly burdensome. I see you shaking your head.

Mrs. CAPPS. Well, I want Ms. Foley to be able to respond to you.

Mr. MELSKI. I hope you are right. But the problem is that the hopes and the opinions are not in the regulations, and that is where we are concerned.

Ms. FOLEY. I actually think I described a couple of multidisciplinary interactions that give an example of the role of the entire treatment team. And it is the provision, coordination and management of health care, including consultations and referrals between health care providers. It does allow—I don't know how the doctor could say nurses change roles. We have a scope of practice and a license, so I am not sure what he is describing. I don't wish to argue that point. The very ability in which we all find our work

settings does not mean it to be more restrictive. It is still very possible to meet the standards and protect the policy.

Mr. APPELBAUM. May I follow up on that? Because I think there is a helpful way of amplifying that.

With regard to the minimum requirement, the regulations say specifically that "minimum necessary" does not apply to disclosures to or requests by a health care provider for treatment. So anything that is treatment-related, health care provider, nurse, physician, or anyone else directly involved in care, this minimum necessary requirement is simply out the window. It is not an obstacle to the transfer of information.

If I can add——

Mrs. CAPPS. Please.

Mr. APPELBAUM. The extent of opposition to the prospective consent requirement is in many respects staggering because it is a minimal requirement that was considerably scaled back from the status quo at the request of many of the entities in the health care industry that are now currently complaining about how extensive the requirement is.

The status quo is that we get consent from all of our patients prior to any release of information—contemporaneous consent, not blanket advance consent. So it is truly a minimal requirement that was designed to minimize costs and burden and ought to be seen in that light. We were doing a little bit toward protecting patients privacy and by no means going overboard in that direction.

Mr. MELSKI. What was said was correct for disclosure; what was said was not correct for use. In other words, the minimum necessary standard as it applies to the use of the information, we have the paradoxical situation where I can disclose the entire medical record to another health care organization, the entire record, and yet as I try and use it within my own organization, to use it the minimum necessary standards applies.

Now that is a tremendous paradox, and in terms of the amount of time—I mean, I understand and respect the consents that are done every day for surgical procedures and so forth; but let me share with you that we also do a tremendous amount of research, and our research consents more closely resemble the notification, and that is, they are many pages long. And we have statistics based upon obtaining consent for research that do take 20 to 30 minutes.

Mrs. CAPPS. Yes. I think we are describing a lot of different things. But if I could, Mr. Chairman, if you will allow me say—and I want Ms. Foley to respond.

Mr. BILIRAKIS. Just in a few seconds, please——

Mrs. CAPPS. I know.

Mr. BILIRAKIS. [continuing] because we have another series of votes, and it would be great to finish up.

Mrs. CAPPS. It strikes me how much education is required in all we are talking about, that whoever is consenting also needs to be apprised of in a setting not conducive to reading nine pages.

But if you would like to give a response, very——

Mr. BILIRAKIS. Very briefly, please.

Ms. FOLEY. Absolutely, Congresswoman.

It does require the exchange of good information, oftentimes done verbally in addition to the written because it does require interpretation and clarification of understanding. If someone is to receive an operative report, I would ask them questions about that procedure; and that is common practice to make sure they understood if because the written word, and oftentimes our medical jargon, does confuse.

Mr. BILIRAKIS. Thank you.

Mr. Buyer to inquire.

Mr. BUYER. Thank you, Mr. Chairman.

Mr. Heird, the comments that you have made in your statement, I want to let you know I agree with when you mention about the unintended consequences, about the scope and complexity of the changes required by HIPAA to implement this in a 2-year timeframe. I want to associate myself with your comments here.

But I am also bothered by such stark differences in testimony about costs. First, HHS estimated that the proposed privacy regulation costs $3.8 billion, over 5 years. Then they update the cost estimate. They think the final rule will cost $18 billion.

Then with regard to the administrative side of the house—this implementation, the administrative simplification, and the transactions and code sets regulation—that somehow is not supposed to cost anything. That is going to save money as I read the testimony of Ms. Goldman. I don't believe that because there are going to be some costs here.

So, Mr. Heird, you are a senior officer here in a very large health insurance company, talk about the costs and implementation here and then give some recommendations to the committee on what we should do as we try to implement this rule.

Mr. HEIRD. Congressman, our views about the cost of the program square with yours. We believe that in our particular case—for instance, Health and Human Services suggested that a large health plan would spend about a million dollars to be compliant with HIPAA and all its dimensions; we are going to spend approximately a hundred times that number. About half of that will be for transactioning code sets.

Mr. BUYER. A hundred million dollars?

Mr. HEIRD. Yes. And about $50 million of that will be for transactioning codes.

And I point out to you that about 70 percent of our claim transactions today are already automated. In other words, they come in in a paperless mode. So from our point of view we do not know where these alleged savings will occur.

The remaining $50 million will be in privacy and security, and so from our standpoint, it is, as I pointed out in my oral testimony to you, pure cost to us. I don't want to say that privacy is an issue because it costs money, but clearly the value will be delivered.

But as we also look at hospitals, we have issued a report, and I would like to suggest the committee see that report yesterday from Tillinghouse Towers Perry where they estimated what the cost would be for the provider industry. The initial estimates for hospitals for transactioning codes alone were between $100- and $300,000. The latest study would suggest that the cost would be

$750,000 to over $3 million to implement just the transactioning codes.

Our thought is that privacy for hospitals will be more expensive than the transaction and code set requirements, so we think that the cost estimates are woefully inadequate and there really will not be savings to offset the cost of desired privacy features.

Mr. BUYER. Mr. Chairman, I would ask unanimous consent that the Tillinghouse-Towers Perry report, as referenced by Mr. Heird, be incorporated in the record.

Mr. BILIRAKIS. Without objection.

[The report follows:]

BLUE CROSS AND BLUE SHIELD ASSOCIATION

Final Report: Provider Cost of Complying with Standardized Electronic Formats

MARCH 2001

EXECUTIVE SUMMARY

While the move to standardized electronic transactions in the health care industry is long overdue, most hospitals and provider organizations are underestimating the magnitude of the challenge—both in terms of time and money. The standardization of transactions and code sets will generate significant financial issues for providers. The changes to provider information systems will affect nearly every aspect of business operation and will require significant coordination across the healthcare industry.

All of this takes time, but time is running out. Under the current rule, wholesale change to the billing platform of the health care industry must be done by October of 2002. The unanswered question is: will the industry be ready to embrace this change without significant reductions in service and a short-term increase in costs as organizations seek and implement remedies?

Study Findings:

- Most provider organizations are underestimating both the investment costs and the time required to comply with standardized formats.
- The migration to standardized codes and loss of unique identifiers and local codes may cause some providers to lose special payment considerations that have been historically negotiated.
- A November 2000 survey of hospitals found that none of the surveyed organizations have completed a comprehensive budget to implement the electronic standards. These results were substantiated by follow-up calls in January 2001.
- Tillinghast-Towers Perrin estimates that it takes roughly five years to generate payback and payback estimates are highly dependent on achieving a significant reduction in accounts receivable.
- These ROI calculations do not account for the potential of significant changes to standardized formats and code sets that may occur during the payback period.

Cost Estimates:

- In the final rule for standardized formats, HHS estimated hospital costs to be $100,000 to $250,000, however Tillinghast-Towers Perrin estimates costs to a mid-sized hospital (200-300 beds) are $775,000 to $3.5 million.
- Costs to teaching hospitals and other integrated delivery systems are $1.5 to more than $6 million per organization.
- Costs to individual physicians are approximately $3,000 to $5,000.
- For a typical 50-physician practice costs could range from $75,000 to $250,00 depending on age and characteristics of the information systems.

FINAL REPORT: PROVIDER COST OF COMPLYING WITH STANDARDIZED ELECTRONIC FORMATS

History

The Secretary of HHS released final rules regarding electronic formats for the health care industry in August 2000. Developed under the auspices of the Administrative Simplification section of the Health Insurance Portability and Accountability Act of 1996, these standardized formats are one in a series of rules that are required

by the Act. Under the regulations, covered entities (health plans, health care clearinghouses, and providers who transmit administrative data in electronic form) will have two years to comply—October 2002. The standard transactions required are:

- Health claims and equivalent encounter information
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health care payment and remittance advice
- Health plan premium payments
- Health claim status
- Referral certification and authorization
- Coordination of Benefits

Under the rule, if a covered entity conducts any of the above transactions with another covered entity (or between covered entities owned by the same parent) using electronic media, the covered entity must use the standard formats adopted by HHS.

In addition to standardized formats, the regulation requires the use of specified national medical code and non-medical code data sets. A code set is any set of codes used for encoding data elements, such as diagnosis codes, and medical procedure codes. In general, the code sets adopted by the Secretary include:

- ICD-9 coding for diagnoses and inpatient services
- CPT-4 for professional services
- CDT-3 for dental services instead of HCPCS "D" codes
- NDC for drugs instead of HCPCS "J" codes

* All locally defined codes are eliminated

Other aspects of HIPAA Administrative Simplification include:

Privacy	Final rule issued December 28, 2000
Security	Proposed rules
Provider Identifier	Proposed rules
Employer Identifier	No proposed rules issued to date
Health Plan Identifier	Proposed rule
Individual Identifier	No proposed rules issued to date

Implementation of all aspects of this first Administrative Simplification regulation is to take place over the coming two years. For electronic formats, all sectors of the health industry wishing to do business electronically must implement the standardized formats and code sets required by HIPAA by October 2002. This timetable will require massive effort and significant investment by hospitals and other health care providers. The alternative is a disruption of existing electronic transactions and a return to the use of paper and telephone transactions.

Hospitals and physicians will be required to make wholesale changes to their information systems that will affect nearly every business operation. And, unanswered questions remain regarding how electronic formats will be implemented. In many cases, business rules to guide how electronic formats will be used have not been developed. Answers to these business rules may have an impact on how providers are paid and the level of payment. The migration to standardized codes, loss of unique identifiers, and elimination of local codes may cause some providers to lose special payment considerations that have been historically negotiated.

Finally, implementation of standardized formats will require significant coordination across the healthcare industry, requiring hospitals, doctors, other health care providers, insurers, HMOs, government and others to coordinate activities.

Hospital And Provider Considerations Regarding Electronic Formats

Tillinghast-Towers Perrin has found that hospitals, physicians and other providers have been slow to recognize the magnitude of migration to standardized electronic formats. Our industry telephone survey of hospital executives conducted in late 2000 found that virtually no hospitals have carefully considered the implications of HIPAA. A typical comment is "our core mission is patient care, not data communications". Subsequent telephone interviews conducted in January, 2001 reinforced this earlier finding and showed that many providers have still done little to prepare. This is consistent with a recent national survey conducted by the Gartner Group which found that "less than 10 percent of respondents have completed or are currently involved in estimating their organizations' expected return on investment for implementing HIPAA-compliant electronic transactions." Many hospital executives have been focused on more immediate concerns such as Y2K, implementation of the outpatient prospective payment system, and reductions in Medicare reimbursement rates.

Standardization of electronic formats will require significant business process change and investment in several components of the organization, including:

- Billing and accounting systems
- Electronic medical records
- Data warehouses
- Electronic data interchange (EDI) systems
- Data translators
- Other information technology

In general, we found that hospital executives are looking to health plans to take the lead in implementing and coordinating the transition to standardized formats. Hence, there has been very little planning around identification of current processes, gaps compared to HIPAA requirements and strategies to address these gaps. In this regard, the timing of format releases and specific questions regarding data content of transaction formats remain open issues. While hospitals are looking to health plans to take the lead in release of formats, they do not feel that they must follow health plan timeframes prior to October 2002.

Cost Estimates for Implementing Standard Electronic Formats

Many consultants and government agencies have attempted to estimate the cost to hospitals and physicians of migrating to standardized electronic formats and code sets. Overall, we have found that most provider organizations are underestimating both the investment cost and the time required to comply with standardized formats.

Costs to develop standardized transaction formats for any particular hospital or provider practice are highly dependent on several factors, including:

- Degree of electronic data interchange already in place and level of current compliance
- Hardware configuration and age of system
- Software packages and degree of integration between business platforms
- Data warehouse capacities
- Use of data translators or clearinghouse functions
- Use of billing agencies and ability of these organizations to comply with standardization within current cost structures
- Other factors

HHS Estimate

The electronic format final rules estimate that average costs to hospitals range from $100,000 to $250,000. Furthermore, HHS anticipates that billing agencies and clearinghouses will offer services that address standardization issues.

Zero-based Budget Estimate

Many health plans and some hospitals are currently budgeting for remediating to standardized electronic formats. A representative budget for a mid-sized hospital (200-300 beds) that is presented below shows that the total technology cost to implement standardized transaction formats and code sets ranges from $775,000 to over $3 million.

Representative Hospital Electronic Format Remediation Budget

Area/Gap	Estimated Cost
Reprogramming billing systems	$100,000 to $1 million
Purchasing a HIPAA compliant data translator (necessary investment for most hospitals)	$100,000 to $250,000
Business office and provider training (new codes, new formats, new identifiers, etc.)	$50,000
Charge slip and charge master (changes in how charge slips are designed and charge masters maintained).	$25,000
EDI upgrade for eligibility and claim status check (migration from non-compliant dial-up systems to new platforms).	$50,000 to $100,000
Consulting (including estimate revenue impact of standardized code sets)	$100,000
Data mapping and data warehouse upgrade (most hospitals must map current transactions to standard formats. Those that operate data warehouses for analytic purposes must revise layouts and map old fields to new).	$100,000 to $1 million
MSO/PPO/PHO remediation (virtually all hospitals now have affiliated organizations that bill on behalf of staff physicians and other organizations).	$250,000 to $1 million
Estimated total:	**$775,000 to $3,525,000**

Teaching hospitals and other integrated delivery systems that include both insurance functions, physician office administration, facilities and ancillary services will require significantly greater investment. Again, depending on the state of the cur-

rent information systems, total costs would be roughly two to three times the averages noted above, or $1.5 million to over $6 million.

Likewise, physicians must upgrade and change internal billing systems, referral authorization procedures and claims status checks. Depending on age and characteristics of the information system, costs could range from a low of $75,000 to a high of $250,000 to remediate for a typical 50-physician practice. For a typical solo physician practice, a retooled billing system would require a $3,000 to $5,000 investment. The upper estimates assume that the current information platform cannot be sufficiently modified and a replacement must be purchased.

Clearinghouses and Billing Agencies

Many organizations are turning to clearinghouses and billing agencies for assistance in meeting the new requirements. In the near term, this solution may seem to be a cost effective and efficient way to meet the October 2002 deadline. However, while these organizations often work on behalf of solo physicians, the introduction of a clearinghouse may not be preferable for high volume providers, hospitals and those providers that wish to maintain direct contact with payer organizations. Additionally, clearinghouses add another "middleman" layer to the health care delivery system. They do not represent a long-term solution to enhanced administrative efficiency.

Transaction costs for clearinghouses reportedly range from less than 5 cents per transaction to approximately 20 cents per transaction. Low cost options depend on very high volumes of transactions, not limited to claims. Other transactions include eligibility checks, referral authorizations, claims status checks and other EDI functions. Depending on the volume of transactions, even at relatively low per transaction costs, the total annual costs are significant.

Finally, it is not clear that most billing agencies and claims clearinghouses are rapidly moving to comply with administrative simplification requirements. Compliance for these organizations requires significant capital investment and time to implement. With less than two years to go, TTP is not aware that any provider clearinghouse or billing agency is HIPAA fully compliant.

Return on Investment Analysis

While the short-term costs are high, many hospital executives are positively disposed to implementation of electronic formats. Since many hospitals already bill electronically over 90 percent of claims, positive ROI is dependent on:

- Increased billing accuracy due to elimination of plan-specific codes
- Reduction of errors due to plan-specific claims formats
- Front-end insurance eligibility verification through a standardized interface with all health plans

Some hospitals anticipate significant one-time revenue increases in the form of reduced accounts receivable due to electronic standardization. One organization anticipates a one-time reduction of at least 10 days in receivables. Others anticipate even greater savings. These reductions would result in a one-time increase in hospital revenues that would help offset standardization costs.

Secondary benefits are also noted by selected hospital financial analysts. Administrative simplification is anticipated to generate a reduction in billing office administrative costs due to rejected claims and other manual processes. This assumes that the standardized electronic formats will reduce billing errors generated by the hospital. Overall, payback for developing the infrastructure to support electronic standardization is anticipated to be within five years.

However, Tillinghast-Towers Perrin has found that many hospitals may be underestimating the cost of migrating to standardized formats. Interviews with hospitals nationwide that Tillinghast Towers Perrin conducted in November 2000 showed that none of the surveyed organizations have completed comprehensive budgets to implement the electronic standards. Among those few organizations that have conducted preliminary ROI analysis, it takes roughly five years to generate payback and payback estimates are highly dependent on achieving a significant reduction in accounts receivable.

Finally, these informal ROI studies do not account for the required changes to standardized formats once they are implemented. In fact, once the mandated formats are fully implemented in two years, it is highly likely that American National Standards Institute will recommend movement to the International Standard Formats that the remainder of the business world is already adopting. The HHS mandated formats are based on a batch mode format standard. In the world of e-business, batch mode has been replace by real-time transmissions. In fact, those dot-com vendors that currently service the health care industry, to comply with mandates, must remediate their internet applications to the previous generation of EDI-

batch mode transmissions. Three years from now, the health care industry will likely be adopting International Transaction format standards, souring positive ROI calculations.

Conclusions

While the move to standardized transactions in the health care industry is long overdue, most hospitals and provider organizations are underestimating the magnitude of the challenge—both in terms of time and money. Additionally, standardization of procedure codes in some markets and for some organizations may generate significant financial issues. For instance, when all local codes are mapped to standard codes, the revenue associated with the standard code will likely be different—either higher or lower, than current payments. While health plans will seek, at a minimum, a revenue neutral solution, for any particular provider organization, payments will change. These unintended windfall gains and losses must be anticipated and mitigated, by both health plans and provider organizations.

All this takes time. And, time is growing short. Wholesale change to the billing platform of the health care industry must be accomplished by October 2002. The unanswered question is: will the industry be ready to embrace this change without significant reductions in service and a short-term increase in costs as organizations seek and implement remedies?

Mr. BUYER. I also ask unanimous consent that—the full committee chairman cited a letter by the President of the American Psychiatric Association, dated March 12, 2001, to the U.S. Department of Health and Human Services—that that letter also be placed in the record.

Mr. BILIRAKIS. Without objection, that will be the case.

[The letter referred to follows:]

AMERICAN PSYCHIATRIC ASSOCIATION
March 12, 2001

U.S. Department of Health and Human Services
Attention: Privacy I
Room 801
Hubert H. Humphrey Building
200 Independence Avenue, SW
Washington, D.C. 20201

RE: American Psychiatric Association technical amendment to the final rule-Standards for Confidentiality of Individually Identifiable Health Information (Federal Register, February 28, 2001, PP12738-12739.)

DEAR SECRETARY THOMPSON: The American Psychiatric Association (APA), a medical specialty society representing more than 40,000 psychiatric physicians nationwide, believes the final privacy regulation is an important first step toward protecting patient privacy. We recognize there is still work to be done to overcome implementation obstacles to achieve compliance if these regulations are to appropriately serve the needs of the American people. At the same time please know that any delay in the implementation date is contrary to the health needs of the American people.

Regrettably, it is often overlooked that confidentiality is an essential element of high quality health care. Some patients refrain from seeking medical care or drop out of treatment in order to avoid any risk of disclosure of their records. And some patients simply will not provide the full information necessary for successful treatment. Patient privacy is particularly critical in ensuring high quality psychiatric care.

Both the Surgeon General's Report on Mental Health and the U.S. Supreme Court's *Jaffee v. Redmond* decision conclude that privacy is an essential requisite for effective mental health care. The Surgeon General's Report concluded that "people's willingness to seek help is contingent on their confidence that personal revelations of mental distress will not be disclosed without their consent." And in Jaffee, the Court held that "Effective psychotherapy depends upon an atmosphere of confidence and trust . + . . For this reason the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment." Accordingly, the APA recommends at the close of the comment period you move forward with the publication of the regulations and not delay the implementation date but rather you use your regulatory authority to respond appropriately in the public interest to protect the privacy of the medical record to the comments received. And

we suggest this notwithstanding our concerns hereinafter expressed that we believe changes in the provisions on mental health records are critically needed to ensure the delivery of effective mental health care, or other comments that may be submitted.

The Administration's efforts seeking comments are commendable, and while the regulations need to take these additional steps, delayed implementation would be more harmful. When you have reviewed all the comments you can then bring the "stakeholders" together, and secure the necessary stronger protections to advance patient privacy which we as physicians believe that our patients and our families need.

The APA urges the following revisions to the proposed regulations:

1) *Section 164.506. Consent for uses and disclosures for treatment, payment, or health care operations. Health care plans, providers, and clearinghouses must be required to obtain an individual's consent before their medical record can be disclosed for treatment, payment, or other health care operations. Patients should be able to choose who will see their medical records.*

The APA is concerned about blanket consent at the time of entry into a health plan. This blanket consent means a patient is authorizing subsequent disclosures of personal information without knowing the type of information allowed to be disclosed, or who can receive this information. While the regulations allow the patient to revoke this consent, the regulations do not protect the patient from being dismissed from the plan for doing so. The patient should have the ability to revoke the consent at any time. The APA feels the rule does not adequately provide this patient protection.

Excessive demands by payers for access to patients' medical information, which often amount to requests for entire patient records, should not be allowed. The demands routinely include information for which there is no legitimate need for payments purposes. Significantly narrower definitions of the information that may be released for payment purposes is needed to protect patient privacy. There needs to be an objective standard for the information that is needed not a subjective standard.

Patients should have the right to consent to—or refuse-participation in disease management programs. In addition, an individual's enrollment or costs should not be affected if he or she declines to participate in a plan's disease management program. We oppose any disclosures of health information for disease management activities without the coordination and cooperation of the individual's physician. Yet, there is no such requirement in the final rule. We believe this term needs to be defined narrowly, in order to prevent inappropriate use and disclosure (for example for marketing purposes) of health information without the patient's consent.

2) *Section 164.512(e). Standard: Disclosure for judicial and administrative proceedings. Patients will lose some existing privacy protections because the current practice of hospitals and doctors, generally requiring patient consent and/or notice before disclosure, will change as a result of the regulation. Patients' ability to decide when their medical record information will be disclosed outside the health system will be reduced.*

For example, currently when hospitals or doctors receive a request for a medical record from an attorney for civil and administrative purposes, they will generally not disclose medical records information without notice to the patient and/or the patient's consent. But the new regulation would allow providers to disclose medical records information to attorneys who write a letter "certifying that the . . . information requested concerns a litigant to the proceeding and that the health condition of such litigant is at issue". As long as reasonable efforts are made to give notice of the request to the patient and to secure a qualified protective order. These procedures provide no check on attorneys' behavior in requesting records of marginal relevance to a case or for the purpose of embarrassing or intimidating opposing parties. Once the information is disclosed, the damage is done; post hoc remedies cannot restore parties' privacy.

3) *Section 164.514. Standard: Uses and disclosures of protected health information for marketing and fundraising.*

The APA is very concerned about a marketing and fundraising loophole that exists in the regulation. A patient's authorization is not needed to make a marketing communication to a patient if: it occurs face-to-face; it concerns products or services of nominal value; and it concerns the health-related products and services of the covered entity or of a third party and meets marketing communication requirements. For example, a marketer could knock on the door of a pregnant woman and try to sell her a product or service. Under the fundraising loophole a covered entity

may use or disclose patient's demographic information and dates of health care to a business associate or to an institutionally related foundation, without a patient's authorization. We are aware the covered entity must include in any fundraising materials it sends to a patient a description of how the patient may opt out of receiving any further fundraising communication. However, the APA maintains that the patient should be able to opt out before the fundraising communication is sent. For example, a commercial fundraising organization for a health facility could use confidential information about a Governor being a patient at that facility without the Governor's consent for use in their fundraising. The APA is particularly concerned about the need for sensitivity with psychiatric patient's names. Commercial fundraisers should not be allowed to take advantage of patients especially those with mental illness.

We strongly believe that personal health information should never be shared for the purposes of marketing or fundraising without the patient's informed consent and are disappointed that the rule only permits such not to occur futuristically. Effectively, an ex post facto withdrawal of consent after the marketing and fundraising damage has occurred. There is an easy solution, merely require the fundraising endeavors to have a patient consent (opt in) before the activity occurred rather than the regulation's authorizing the patient to opt out of any further fundraising endeavors.

4) *Section 164.508. Use and Disclosure for Treatment, Payment, and Health Care Operations-exception for psychotherapy notes.*

Additional protections consistent with the Supreme Court's Jaffee v. Redmond decision for mental health and other particularly sensitive medical record information are essential. Without such additions the protections essential for effective mental health care will be lost.

We believe that all medical records should enjoy a level of protection so that no additional protections are needed for psychiatric or other sensitive information. In fact, the U.S. Supreme Court recognized the special status of mental health information in its 1996 *Jaffee v. Redmond* decision and ruled that additional protections are essential for the effective treatment of mental disorders.

APA believes that the rule allows for the use and disclosure of far too much information without the patient's consent. We also believe that language needs to be added to clarify that the amendment's privacy protections cover treatment modalities broader than psychotherapy (and indeed virtually all psychiatric information) and also cover information that is part of the patient's medical record.

The regulations change the current standard of practice relevant to the psychotherapy documentation. There is a new requirement for keeping a second set of records, which most psychiatrists do not now do, and which will result in increased time, difficulty, and cost associated with record keeping.

5) *Section 160.203. Standard: Disclosure for law enforcement.We also want all Americans to be free from unreasonable police access to their most personal medical record information. The Administration's proposal falls short in this area.*

Under these regulations law enforcement agents would simply issue written demands to doctors, hospitals and insurance companies to obtain patient records, without needing a judge to review the assertions. We are also very concerned by the separate provision that would allow for the release of medical record information anytime the police are trying to identify a suspect. This broad exception would allow computerized medical records to be sifted through by police to seek matches for blood, or other health traits. In addition, the provision that allows disclosure on the basis of an administrative subpoena or summons, without independent judicial review, is particularly troublesome.

We believe that the same constitutional protections (a Fourth Amendment probable cause standard including independent judicial review for all requests) should apply to a person's medical history as applies to their household possessions.

6) *Section 164.502. Business Associate Provisions. Section 164.300. Compliance and Enforcement.*

The business associate provisions of the proposed regulation result in overly broad physician liability, and the regulations also need to be reconsidered in light of the need to limit the administrative burden on physicians who practice independently or in small practices.

The rule identifies most health care related entities other than physicians, providers, health plans, and health data clearinghouses as "business partners" of physicians, which could only be held to the confidentiality standards of the regulation through contracts with the covered entities, such as physicians. In essence this enor-

mous regulatory framework will be achieved largely through the inappropriate liability placed upon physicians.

A covered entity will have a new duty to mitigate any known harmful effects of a violation of the rule by a business associate. This duty may, in effect, compel covered entities to continue to monitor activities of business anyway. It is not clear if a psychiatrist, for example, could be held accountable for prohibited activity by its business associate, even if the psychiatrist **should have known** of the prohibition. For purposes of the rule, actions relating to protected health information of an individual undertaken by a business associate are considered to be actions of the covered entity. Therefore even though covered entities may avoid sanctions for violations by business associates if they discover the violation and take the required steps to address the wrongdoing, they may be vulnerable to a negligence action. APA believes these provisions present the potential for overly broad liability for physicians who, themselves, are complying with the regulation's requirements.

It is not unreasonable to expect that some additional burdens will fall on physicians as part of efforts to increase patient privacy. However, the level of administrative burden currently contained in these regulations is not equitably distributed. Particularly important is expanding the concept of scalability so that the administrative burden on physicians in solo or small practices will be manageable, taking into consideration their limited resources and staffing.

As noted above, the regulatory framework of this regulation relies too heavily on physician liability (via business associates). If indeed it is the framework by the Secretary that is enacted through regulation or through congressional action, we could not support providing individuals with a private right of action.

7) *Section 164.512 (k). Standard: Uses and disclosures for specialized government functions (Military, State Department and others).*

The special rules in this section are overly broad and do not provide adequate procedural protections for patients. Except in very narrow circumstances the consent of the individual should be the rule for the use and disclosure of governmental employees' medical records information. We also note that intelligence agencies and the State Department are not even required to publish a rule, subject to public comment, defining the scope and circumstances of their access to medical records. Particularly objectionable are the provisions allowing broad access without patient consent for use and disclosure of medical records of Foreign Service personnel and their families.

8) *Volume 65 Federal Register page 82790. Costs: The APA believes the estimated costs imposed on small psychiatrist's offices for the first year of $3, 703 and consecutive years of $2,026 seem unrealistically low.*

Psychiatrists will experience significantly higher costs and will have a heavy administrative burden, such as getting satisfactory assurances from a business associate through a written contract, keeping psychotherapy notes separate and locked from the rest of the psychiatric record, and providing written notice of their privacy practices to their patients. Similar to small health plans, small physician offices should be allowed to have 36 months for compliance to spread the cost over a longer period of time.

9) *Section 164.530 Administrative requirements.*

A clarification is needed on the privacy official provision. For example, can a psychiatrist who does not have any staff serve as the privacy official? If a privacy official makes a mistake will only the privacy official be liable?

10) *Section 160.104 Modifications.*

The APA believes implementation should not be delayed because the Secretary has discretion under section 160.104 to adopt a modification to a standard every twelve months and the provision expressly allows modification within the first twelve months after the effective date.

11) *We welcome the many very positive provisions contained in the regulation and urge that they be retained including:*

- the general rule of non-preemption of more privacy protective state laws (Section 160.203)
- a higher level authorization is required for any use or disclosure of psychotherapy notes, and most importantly psychotherapy notes may not be disclosed without the patient's specific authorization (Section 164.508)
- the requirement that the entire medical record not be used in cases where a portion of the record will suffice, i.e. the "minimum amount necessary" require-

ment. Physicians can cite this provision when dealing with unreasonable health plan requests for information. (Section 164.502 (b))

- the requirement that an entity must notify enrollees no less than once every three years about the availability of the notice and how to obtain a copy of it (Section 164.520)
- extension, in many circumstances, of federal "common rule" research protections to privately funded research (Section 164.512)
- the right to request restrictions on uses or disclosures of health information (such as requesting that information not be shared with a particular individual) (Section 164.522)
- the right to request that communications from the provider or plan be made in a certain way (such as prohibiting phone calls to individual's home) (Section 164.502)
- the right to inspect and copy one's own health information with the exception of psychotherapy notes and when the access is reasonably likely to endanger the life and physical safety of the individual or another person (Section 164.524)
- the patient needs to be provided documentation on who has had access to this information and the right to request amendment to the record if it contains incorrect information (Section 164.528)

In conclusion, we believe the privacy regulations are very much needed but at the same time (as above noted) believe some provisions are inadequate to protect our patients. Yet, our gravest concern is that certain parties which were disappointed at how protective these regulations are of patient privacy will in support of their own interests be arguing for surrendering many of the protections that patients have just gained. In order to insure interested stakeholders regulatory comments do not diminish medical record privacy protections we recommend that the Secretary not only receive all interested stakeholders (such as insurers, providers, health care clearinghouses, and consumer groups) comments, but also convene a meeting of the interested stakeholders as soon as possible after the conclusion of the regulatory comment period BUT before publication of the "new" final medical record privacy regulations.

Secretary Thompson we agree with you to conclude April 14, 2001. We of course encourage the Administration to stand firm on these issues and support strong protection of medical record privacy.

Thank you for considering our views, and we look forward to discussing them with you further. Please feel free to contact Jay Cutler, Special Counsel and Director Government Relations or Nancy Trenti, Associate Director, at (202) 682-6060.

Sincerely,

DANIEL B. BORENSTEIN, M.D., *President*
American Psychiatric Association

cc: Anne Phelps
Mitchell Daniels
Sally Canfield

Mr. BUYER. I yield the balance of my time to Mr. Norwood.

Mr. NORWOOD. I thank my colleague. I have a minute or 2 here.

I want to ask a question that is probably too late to ask, but I am curious. How many of you feel we should have a Federal standard to cover privacy? Just do like that so I can see.

Everybody agrees we should not worry about the States and just have Federal coverage that is uniform?

Mr. APPELBAUM. No.

Mr. NORWOOD. Well, respond, Dr. Appelbaum.

Mr. APPELBAUM. Dr. Norwood, the States have been historic regulators of health care in this country, and have, in that role, initiated many of the experiments that later evolved into national policies.

State regulation is a day-to-day reality in health care. Physicians are licensed by their States, hospitals are licensed by their States. Medicaid is a State program, and the industry is used to operating within the confines of State legislation. That is the status quo.

To the extent that States decide that for their citizens they would like to provide a higher level of privacy protection, and their citizens agree, we think they should——

Mr. NORWOOD. Thank you. I understand.

In other words, you want a Federal law that is the bottom line, and then you want the States to be able to add to it in whatever manner they see fit?

Mr. APPELBAUM. That is correct.

Mr. NORWOOD. I have got reams of paper up here from a lot of people who object to this particular regulation on different grounds. People have different thoughts as to why it is not right.

A lot of you have objected to this regulation too, and even those of you who want to see this rule effective have pointed out this is not efficient, it is not perfect. It has a lot of flaws, but let's go ahead with the rule, some of you say, and then we will worry about correcting it a little later.

Now, that gives me some pause for thought. If you are trying to say to us, okay, in the next 23 days let's perfect this rule so it really does work and let's take care of the concerns that all of you have, that all of these people have, I would tell you that we can't do it within 23 days, I don't believe. Nothing up here moves very fast. And my suggestion to you is that we pass rules and regulations in this town all the time that have unintended consequences, that come back to bite us, that are way too expensive, that simply do the opposite of what the rules set out to do. Why in the world on something this important wouldn't we try to get this right before we have a rule?

I understand there is 2 years to comply. I understand the Secretary—staff says different, but some of you say that the Secretary within a year could get in and fix it. Why in God's name put a rule in place we know is wrong? And you have all pointed out, I think, many areas where it is wrong.

And, incidentally, Mr. Chairman, I have a simple letter with unanimous consent I would like to offer for the record. It is from the American Medical Association, and if we could, I would like to have that put into the record.

Mr. BILIRAKIS. Can you identify it by date?

Mr. NORWOOD. Yes, February 28, 2000, and it is from Dr. Andy Anderson, Jr., M.D.

Mr. BILIRAKIS. Without objection, it will be made a part of the record.

[The letter referred to follows:]

AMERICAN MEDICAL ASSOCIATION
February 28, 2001

The Honorable TOMMY THOMPSON
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

DEAR SECRETARY THOMPSON: The American Medical Association (AMA) appreciates your willingness to provide an opportunity for additional comments on the final privacy regulation recently issued by the Clinton Administration (65 Fed. Reg. 82472) as authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Your decision properly reflects the complexity of the rule and the potential for unintended consequences that are now being identified. We believe that significant changes to the rule are necessary to adequately protect patients and to

make certain portions of the regulation workable before it is implemented. We respectively request a limited extension of the effective date so that new comments can be evaluated and improvements to the rule can be effectuated before the compliance period commences.

Patient privacy is fundamental to the physician-patient relationship and a right long advocated by the AMA. Physicians and other health care providers are the guardians standing between patients and the unrestricted use and access to patients' private medical records. We believe that preservation of patient trust and autonomy in an increasingly technological health care environment is imperative to continue high quality patient care that is expected in this country.

We commend the Department of Health and Human Services for the tremendous work it took to write the final regulation. In fact, we were pleased to see certain improvements from the proposed regulation. However, many serious problems remain and others have surfaced from new requirements in the final rule.

For example, although we are pleased with the new requirement for health care providers to obtain consent before a patient's protected health information can be used for routine matters, the final rule inappropriately exempts health plans from its requirement. Some aspects of the consent requirement also appear to be unworkable without certain modifications. In addition, law enforcement will have virtually unfettered access to protected health information without patient authorization and without a court order. There are also significant loopholes that allow the use and disclosure of protected health information for marketing purposes.

Mr. NORWOOD. If any of you believe that we can correct this rule within the next 23 days to solve problems, almost every one of you pointed out, just give me—let the record show, nobody believes we can do that.

Why don't we just step back here a little bit and try to get this right?

Part of what, really, I am trying to understand is this rule puts so much on us, on the health care provider—Ms. Foley and Dr. Appelbaum and others. I am not aware that there is a privacy problem in this country with the physician, the nurse, the dentist, et cetera, et cetera. I just do not think that is where the privacy problem is. But we put all of this on their back.

And, Ms. Goldman, you know, you are saying this consent form isn't but nine pages, and we may not use that anyway, but the Federal Government has never put out a form that was short and they are not going to start now. And if you don't believe me go to any agency and pick one. They are all burdensome at the very best.

So why cannot all of us just simply agree—I know this has been worked on a long time. Let's step back, give this new Secretary some time, give us some time to address what I consider very legitimate problems. And at some point, perhaps this year, we can make this rule effective and then have the 2 years for compliance and the year for the Secretary to go in and alter where we have made mistakes.

But, Mr. Chairman, please, let's don't make a rule that we know has so many problems in it right now.

And if there is anybody out there that can explain to me my problem with understanding—well, I have got 36 seconds. I would like to know if any of you believe the problem in privacy happens to be with the health care provider. Does anybody believe that is where the privacy problem is?

Let the record show, nobody does. I will yield back.

Mr. BILIRAKIS. The Chair now yields to Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. I will be as quick as I can. It does seem like it is so much effort when really all we want

our insurance carriers to do is pay it, but do not share that information. It seems so simple.

Dr. Melski, your testimony, one of things that concerns me is, I have a district in Houston, Texas. We have a low immunization rate. We work with our immunization coalition. We do an Immunization Day every year. We use our hospital district. We use our city of Houston health department. We use our county health department, and they provide immunization in our district.

Your testimony would say that it would limit it, but the way the practice is now, there is already information provided to parents; and in my area, it is bilingual—Spanish and English—to those parents. Why would it be so difficult to provide something else—and the CDC requires providers to keep records of those vaccines right now. Why would it be hard for them to keep records of that consent?

Mr. MELSKI. Thank you for addressing that, because all these minor points are hard to cram into 5 minutes.

There is currently an exemption for public health, but what we have found in Wisconsin with a project we initiated, an early childhood immunization network, is that the cooperation between the public and private sector is where you really raise the immunization rates, and you have to share information between public health and private.

But in the private sector these consent forms would then have to be enforced. See, the public health has been exempted in them, but the practitioner has not. And so it is just paradoxical.

Mr. GREEN. Maybe that is why we do not use private practitioners. We use public health agencies to provide that.

Mr. MELSKI. Right. What happens is, if you really want to get the kids immunized, you have to get them when you have got them. When they come in for health care into our organization and we have records that we share with the public health nurses——

Mr. GREEN. But you are required by law to share the immunization record, aren't you, with the State health department, because we have created a registry for so many of our States for immunizations?

Mr. MELSKI. Right. But then the question would be—is whether—see, that is part of the problem with these regulations, that some people that are in favor of them sort of have this positive interpretation that, okay, in that area we don't have to have a consent.

Mr. GREEN. That is the problem with any regulation, that is, somebody's way to interpret it. And hopefully, whether you are a provider or health care, insurance carrier or someone else——

Mr. MELSKI. It is only the foot in the door. The real issue where we can really save lives is if we could share preventive information on mammograms, prostate exams, colon exams and so forth; and the ability to share that information among all providers would save lives.

Mr. GREEN. Okay. With the permission of that person. I really don't want my colon scope to be sent out on a Christmas card unless it is with my written permission and greeting with it.

Mr. MELSKI. It is true. The problem with immunizations and a lot of preventive health and research for that matter, is it is always

good if everybody else agrees to do it except you. It is true for immunizations; it is certainly true for research.

Mr. GREEN. Again, I understand that. But on immunization, like you said, public health has an exception, but for my own records, you still should have my permission to share that.

Mr. MELSKI. And we do require that for immunization, but it is not nine pages, single-spaced. When you talk about consents for surgery that are two pages long, and now you have a nine-page consent for a sore throat or a nine-page consent for immunization.

Mr. GREEN. I haven't seen a nine-page consent, but having signed those consents for minor surgery, I think we could probably—and I am sure the Secretary, hopefully before this month is out, there would be an effort to reduce that to something and also in lay language. If it is nine pages, obviously ten lawyers drafted it.

Mr. MELSKI. Right. And technically it is notification that has to be referred to in the consent. But still it is the whole implication of what is our obligation before we can carry out some of these very important tasks.

Mr. GREEN. Again, that is what HHS is there for.

Thank you, Mr. Chairman. I yield back.

Mr. BILIRAKIS. I thank the gentleman.

Mrs. CAPPS. Mr. Chairman, could I ask unanimous consent so that members of the committee may have a week to submit questions to these witnesses?

Mr. BILIRAKIS. Yes, by all means. Of course, I have already mentioned that.

I know that you are willing to respond to those questions. It has been quite a hearing and you have made it so. It is important that we have this knowledge. It is also important that HHS has this knowledge. Hopefully the right thing will be done. I know the bottom line is, we all want some sort of privacy protection.

Thank you very much. The hearing is adjourned.

[Whereupon, at 1:50 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF ROBERT C. LOWER, ALSTON & BIRD LLP

Mr. Chairman and distinguished members of this Committee: My name is Robert C. Lower. I am a partner with the law firm Alston & Bird in Atlanta, Georgia, where I lead a group of lawyers who focus on health care law and health care privacy. I appreciate this opportunity to share with the Committee my personal observations regarding the impact of the HIPAA privacy regulations, as well as some thoughts on how those regulations could be improved.

Let me start by saying that the health care community is committed to the confidentiality and security of personal health information. In almost 30 years of practice, I have observed countless instances where medical practitioners and the management of health care facilities have demonstrated their determination to protect the privacy of patients. I believe that the thousands of companies and millions of individuals who are part of the best health care system in the world are protecting, and will continue to protect, the confidentiality and security of Americans' personal health information under existing confidentiality laws.

I also believe that the Department of Health and Human Services (HHS) should be commended for the hard work that went into the HIPAA regulations and for their good intentions in pursuit of the protection of medical records. However, as outlined below, I have a number of practical concerns about the HIPAA privacy regulations. I believe they are fundamentally flawed and *must* be revised.

Bureaucratic overload

HHS created the HIPAA privacy regulations with virtually no legislative foundation and, unfortunately, the regulations are a textbook example of regulatory excess. From time to time, I advise clients in other industries, including e-business and financial services, on privacy matters and I am struck by the contrast between the HIPAA rules and, for example, the rules issued by the financial services regulatory agencies under the Gramm-Leach-Bliley Act. That law addresses the privacy of another type of highly sensitive information, namely, personal financial information. In comparing the two sets of regulations, it is interesting that the rules issued by HHS have an aura of suspicion about them, as if the writers distrusted the intentions of the entire health care industry. Why else would HHS create such detailed rules, and provisions like the "minimum necessary" requirement, that appears to be premised on the notion that health care professionals cannot be trusted to collect and use information appropriately in order to deliver first class health care?

I am concerned that the HIPAA regulations will interfere with the convenient and flexible delivery of health care, curtail the free flow of information for medical research and health care quality management, and impose huge costs on the health care system without corresponding benefits to consumers. By micro-managing the collection and use of personal health information, HHS is substituting its bureaucratic judgment for the business judgment and the innovative creativity of the health care community.

Costs and administrative burden

As just noted, the HIPAA regulations will impose enormous costs and administrative burdens on health care providers, health plans and health care clearinghouses. The requirements to obtain affirmative consents prior to rendering care, to respond to requests for individual restrictions on the disclosure or amendment of personal health information, and to provide a grievance procedure places major system burdens on the health care system.

I am not an economist but, based on my experience, HHS greatly underestimated the cost of compliance. I know that in drafting HIPAA implementation plans for clients during the past three months, I have been dismayed by the enormous number of changes to systems, policies and procedures, training, patient communications, and compliance programs that these regulations impose on businesses large and small. These changes will cost a lot of money—far more than HHS estimated—and will be passed on in some combination of higher health care costs or reduced benefits.

Minimum Necessary

The HIPAA regulations require that when using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to request, collect, or use only the "minimum necessary" protected health information to accomplish the intended purpose. This requirement does not apply with respect to disclosures to or requests by a health care provider for treatment, for disclosures required by law and certain other disclosures.

I find this provision troubling for several reasons. First, as noted above, it appears to reflect a suspicion that health care professionals collect and use personal health willy-nilly, for no valid reason. Moreover, the "minimum necessary" requirement is not even mentioned in the Act which raises the question of HHS's statutory authority to adopt this requirement. The cost of this requirement is also a major concern. By the HHS's own estimate, compliance with this will cost $5.8 billion—roughly one-third of the estimated cost of compliance for the entire privacy regulation.

Finally, in my view, the "minimum necessary" requirement has the potential to be "maximum dysfunctional" by adding unnecessary administrative red tape to payment processing and health care operations. Even though the rule allows for routine uses to be defined and general protocols to be developed to facilitate the minimum necessary determination, it will be very difficult to define parameters for requests for information from health care insurers and other payers. Each patient encounter is different, and the information necessary to process a claim for payment will vary depending on the medical condition involved, the terms of the health insurance coverage, and the medical history of each patient. For non-routine uses or disclosures, a minimum necessary determination would be required for each use or disclosure. Likewise, health care operations will be impaired by the requirement. Activities involving patient care information, such as peer review, quality assurance, mortality and morbidity studies and medical education do not involve patient treatment directly and, therefore, will require that a minimum necessary determination be made

for each use and disclosure of protected health information involved in those complicated processes.

I also question the need for the minimum necessary requirement in the context of health care payments. Health insurers already are required by state insurance law to maintain the confidentiality of medical records and to utilize only the information that is "reasonably necessary" for enrollment or payment purposes. In addition, the transactions standards under development by HHS will specify the items of information necessary to process health claims under the requirements applicable to health claims attachments. When the items of information are specified as part of the transactions standards, it will be unnecessary to impose a minimum necessary requirement on the parties involved in the claims process.

With regard to health care operations, I am concerned that the minimum necessary requirement will unduly impair the delivery of healthcare. Patient care information is vital to carrying out peer review, quality assurance, statistical studies, and medical education activities. Confidentiality laws already protect medical records in every state. Imposing a minimum necessary requirement on those activities will affect the quality of care and is unnecessary. I recommend that with regard to health care operations, the standard be changed to permit the disclosure of information that is "reasonably necessary" for a particular purpose. Such a requirement would be far less burdensome, would be flexible to accommodate the wide variety of activities and would provide adequate protection for the privacy of protected health information.

Regulation of "business associates"

The HIPAA privacy regulations impose new requirements on thousands of companies and individuals that do business with covered entities. HHS's goal, namely, to complete the circle of protection for personal health information, is commendable but flawed. The requirements imposed on business associates—including writing policies and procedures, keeping records of disclosures, providing access to personal health information, and making amendments upon request—are unnecessarily burdensome.

In addition, I question the appropriateness and the fairness of attributing the behavior of a business associate to a covered entity for purposes of determining compliance with the HIPAA regulations. I suggest that the regulations be clarified to ensure that a violation by a business associate cannot be used by the Secretary as a basis for an enforcement action against a covered entity.

Consent before treatment

The requirement that health care providers obtain consent before treating an individual is unnecessary and will interfere with the efficient and convenient delivery of health care. For example, under the final regulation a pharmacist could not permit a relative or friend to pick up medication for a sick person unless the patient had consented in advance.

State medical record confidentiality laws and professional ethical principles have protected the privacy of personal health information in the treatment setting for many years. The new regulation will be very costly to implement and will not significantly increase the protection of personal health information.

Thank you, Mr. Chairman and members of the Subcommittee, for providing this opportunity to share my views.

PREPARED STATEMENT OF THE AMERICAN ASSOCIATION OF HEALTH PLANS

The American Association of Health Plans (AAHP) is the principle national organization representing HMOs, PPOs, and other network based health plans. Our member organizations arrange for health care services for approximately 140 million members nationwide. AAHP and its members have long been committed to protecting the confidentiality of personal health information. AAHP's members are "covered entities" for purposes of the HIPAA privacy regulation that has been issued by the Department of Health and Human Services (HHS). Consequently, AAHP's member plans are directly affected by the HHS regulation.

AAHP continues to support uniform federal standards that encourage patients to communicate openly and honestly with their physicians, while at the same time ensuring that health information vital to helping patients get the care they need when they need it continues to flow freely among entities that are responsible for providing, coordinating, and paying for health care. AAHP believes that it is possible to meet the dual goals of maintaining the confidentiality of personal health information and permitting information to be used to perform essential functions. While the final regulation has been improved from its proposed form in many areas, AAHP

believes further improvements are necessary to meet these dual goals. The concerns discussed here are among AAHP's most significant. We will be submitting formal comments to HHS highlighting more thoroughly our comments on the final regulation during the additional comment period recently provided by HHS.

Consent:

AAHP fully supports the final regulation's provision that permits health plans to use and disclose protected health information for the essential, routine activities of treatment, payment, and health care operations without separate patient consent. The department recognizes plans' need for protected health information to perform their essential health care functions. However, AAHP is concerned that the final regulation requires providers to obtain consent for these same routine functions. This bifurcated consent approach is a complete reversal from the proposed regulation, which allowed both plans and providers to use protected health information for routine purposes without separate consent.

Today, physicians and health plans work together to organize care for patients. As a practical matter, health plans depend on providers to supply health information about plan members which often times is not provided through claims data. The final regulation creates obstacles to patients getting preventive care by requiring physicians to have patients fill out paperwork (consents) that will let the providers share that information with health plans. The information is critical, for example, to making sure that a person with diabetes gets annual eye exams to prevent blindness. If the paperwork isn't done exactly right, is missing, or runs into some other problem, the patient may not get the care they need when they need it. This conflicts with a recent Institute of Medicine report that identifies the lack of coordination as one of the big problems in American medical care. These rules would make that problem worse, not better.

AAHP is concerned that the new consent approach will have significant consequences on health plans' ability to obtain critical patient information needed to conduct certain health care operations activities. Again, unless the provider obtains adequate consent, plans may not have the necessary information at their disposal.

If a health plan cannot obtain health information about its members, it cannot perform essential health care operations required by purchasers or private accreditors, such as reporting HEDIS measures and conducting quality assurance and utilization management activities, all of which are essential to ensuring quality care.

Preemption:

AAHP recognizes that HHS has limited authority to change the statutory mandate of HIPAA with respect to the preemption of state privacy laws. However, we would like to take this opportunity to reiterate our support for confidentiality standards that recognize that increasingly, health information moves across state lines—whether from one physician to another for consultation or from a physician to a claims processor in a neighboring state. The dual state and federal regulation created under the final privacy regulation poses significant confusion for consumers and compliance issues for covered entities. The final regulation layers a new comprehensive set of federal rules on top of an already existing complex patchwork of state privacy laws.

AAHP is concerned that the inconsistent demands of state and federal privacy laws under the complex construct of the HIPAA regulatory model will create more red tape and frustration for health care providers and consumers. 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. Instead of facilitating health plan members knowledge of their privacy rights, this complex regulatory framework is sure to confound individuals.

Unanticipated Consequences for Consumers:

In addition to being concerned about the bifurcated consent structure and preemption, AAHP is concerned about unintended consequences the final regulation creates that we are only beginning to identify and that will have a direct impact on care provided. For example, pharmacists are extremely concerned that they will not be able to fill or refill prescriptions for consumers, and prescriptions called in by physicians will not be filled, unless a written consent is on file at the pharmacy. This will create delays for patients, for parents with sick children, and others who will have to come to the pharmacy to sign consents before the pharmacist can fill or refill a prescription. Elderly and disabled individuals will have to obtain and sign a written consent form and somehow deliver it to the pharmacist before anyone can pick up their prescriptions for them. While the creation of such consequences were surely inadvertent and unintended when the final regulation was being developed,

other similar examples will undoubtedly surface as covered entities begin to implement the final regulation and encounter other practical limitations.

We need only look to the experience in the states to see how unintended consequences have arisen. In some of the states that have gone ahead and enacted comprehensive privacy laws, we've seen a number of unforeseen consequences that, in some cases, have caused states to repeal or amend their laws. In Maine, for example, florists were unable to deliver flowers to hospital patients. In Hawaii, the state's workers' compensation program had to be shut down for three months in order to collect patient authorizations. And, in Minnesota, researchers were unable to conduct meaningful medical records research because not enough patients were mailing back their permission forms. These are real examples of what occurs when the flow of information is restricted between and among covered entities who need information to conduct routine, quality enhancing activities for patients.

Treatment of Existing Protected Health Information:

Another key issue is the application of the regulation to protected health information created or collected even before the compliance date of the regulation. As a result, providers will be unable to use information they already have unless they've obtained patient consents. In states where patient consent is not required for treatment purposes (for example in California), providers will have to go back to all of their patients and obtain consent to use the information they already have and have been using all along in order to be in compliance with the regulation. The task of obtaining consent forms from over 200 million Americans within the two year compliance date is a staggering problem that could interfere with everything from refilling routine prescriptions as discussed above, to sending out reminder notices about appointments, medication compliance, etc.

Moreover, given health plans' reliance on providers for patient information to conduct quality improvement and other activities, the impact of this issue will be felt throughout the health care system.

These are just a few of AAHP's concerns with the final HIPAA privacy regulation. Further concerns will be expressed in our comment letter to HHS on the final regulation. We appreciate the opportunity to submit written testimony before the Subcommittee on this very important issue.

AMERICAN ASSOCIATION OF OCCUPATIONAL HEALTH NURSES INC.
March 26, 2001

Honorable MICHAEL BILIRAKIS
Chair, Energy and Commerce Health Subcommittee
The Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Attention HHS Privacy Regulations Hearing March 22, 2001

DEAR REPRESENTATIVE BILIRAKIS: On behalf of the American Association of Occupational Health Nurses Inc. ("AAOHN"), I would like to thank you for the opportunity to provide written comments to the March 22 hearing record on the Final Rulemaking released by the Office of Assistant Secretary for Planning and Evaluation, Department of Health and Human Services ("HHS"), regarding standards for privacy of individually identifiable health information.

AAOHN, a 12,000-member professional association, is dedicated to advancing and maximizing the health, safety, and productivity of domestic and global workforces by providing education, research, public policy, and practice resources for occupational and environmental health nurses. These nurses are the largest group of health care providers serving the worksite. As health care providers, we are committed to ethical standards that place a high priority on maintaining the confidentiality of the individually identifiable health information contained in the medical records that we create and/or maintain as an integral part of our jobs.

We know from first-hand experience that our members' clients—employees across the country—are especially concerned about the confidentiality of the health information available to employers through their operation of employee health benefits plans and occupational health departments. Workers are afraid their companies will use health information inappropriately when decisions are made about hiring, job placement, promotion and firing.

Unfortunately, we also know from first-hand experience that workers' fears are sometimes warranted. The HHS rule represents a significant first step toward health privacy in the workplace, particularly because of the protections it creates for health information heretofore available to employers through their sponsorship

of employee health benefits plans. Still, the rule does not do enough to eliminate employees' risk of inappropriate health information disclosures to their employers because it does not adequately protect occupational health information. As a result, many employers will continue to have relatively free access to personal health information obtained through fitness-to-work examinations, occupational safety and health initiatives, and workers' compensation programs.

The HIPAA statute itself limits the definition of "covered entity" to health care providers who engage in the statute's standard electronic transactions. Neither the statute nor the rules designed to implement it apply to the majority of occupational health care providers because they do not bill third-party payers for their work. Thus, the rule fails to support the professional responsibilities of occupational health professionals who are ethically bound to keep health information on employees confidential.

AAOHN recognizes that employers do have legitimate needs to have access to certain health information for managing workers' compensation or other benefits, accommodating a disabled employee, or assessing an employee's physical capability to complete assigned tasks. However, this does not mean that an employer should have unfettered access to unrelated information—such as an employee's diagnosis or entire medical file.

Additional legislation is needed to authorize the development of privacy rules that will draw the privacy lines appropriately for information collected and used in the work environment. Extending coverage to all health care providers would close the gap in protections for occupational health information in the work environment, preventing the possibility that it will be used in making determinations about hiring, firing or promotion. Without additional legislation, misuse of much personal health information in the work environment will remain unchallenged.

Despite the statutorily required shortcomings of this rulemaking in protecting all occupational health records, *it is imperative that the implementation of the rule not be delayed.* AAOHN believes that you have the authority to make refinements to the final rulemaking without undue delay of these regulations. These new privacy regulations are a major step towards protecting the health and medical information of Americans. It is time to move forward and devote our energy, time, and resources toward implementing the Privacy Rule, rather than wasting precious resources debating whether the regulation should even take effect.

Should you need additional information related to our comments, please feel free to contact me at 770-455-7757 ext. 104 or by email at kae@aaohn.org. Thank you in advance for your thoughtful consideration of these comments.

Sincerely,

KAE LIVSEY
Public Policy and Advocacy Manager

GENERAL COMMENTS ON THE RULE

Overall, the American Association of Occupational Health Nurses (AAOHN) believes that the final standards for the privacy of individually identifiable health information ("Privacy Rule"), published December 28, 2000, constitute a significant step towards restoring the public trust and confidence in our nation's health care system and should be implemented without delay.

Sec. 164.534

AAOHN strongly supports maintaining the current effective date of the Privacy Rule. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated that regulations governing the privacy of health information be promulgated by February 2000. These privacy standards are long overdue, already have been thoroughly debated, and should be put into effect promptly.

For well over a decade, policy makers have recognized that there is a need for a federal law protecting the privacy of health information. Federal protections for health information were included in every proposal on health care reform in the early 1990's.

The rule-making procedure up to this point has been a lengthy and thorough, yet orderly, process. HHS employees spent almost a year reviewing, analyzing, and crafting responses to the comments that the agency received on this rule. The thoroughness with which HHS considered these comments is reflected by the fact that almost 200 pages of the preamble to the final regulation are devoted to summarizing and responding to these comments.

As to assertions that the Privacy Rule should be delayed because some of its provisions are "ambiguous," AAOHN understands that there are *always* interpretative issues when any major rule is adopted. These issues properly are resolved by the agency's issuing guidance on the regulation *after it has taken effect.* The Privacy

Rule is no exception to this general procedure. The purported ambiguity of isolated provisions does not Justify delaying the effective date of the entire Privacy Rule.

To the extent there are legitimate implementation issues that cannot be remedied through the issuance of guidance, HIPAA expressly provides a mechanism for resolving these difficulties *after* the Privacy Rule becomes effective. Under Section 262 of HIPAA (adding Section 1174 to the Social Security Act), the Secretary has the authority to modify the privacy standards during the first 12 months after the standard is adopted (i.e., becomes effective) when such modification "is necessary in order to permit compliance with the standard." Thus, HIPAA anticipates and provides a statutory mechanism for resolving implementation problems after the regulation becomes effective.

Sec. 164.502 and Sec. 164.504

We strongly support the requirement that covered entities receive satisfactory assurance that their business associates will properly safeguard protected health information before either disclosing this information or allowing a business associate to receive protected health information on their behalf Absent such a requirement, covered entities could easily circumvent the Privacy Rule merely by contracting out their business functions. Furthermore, these restrictions properly expand, albeit in an indirect fashion, the protections of the Privacy Rule.

Ideally, a health privacy law or regulation would impose restrictions directly on all health care providers, regardless of their involvement in HIPAA standard transactions, and to those who receives protected health information, including the agents and contractors of health care providers and health plans. Unlike health care providers, these downstream users and processors often do not have an ethical obligation to maintain patient confidentiality. AAOHN recognizes, however, that the proposed regulations were unable to directly cover all health care providers and these organizations due to the Secretary's limited authority under HIPAA. Regulating the agents and contractors of covered entities indirectly, through the covered entities, makes sense in these circumstances. This is particularly true since many covered entities already enter some form of contract with their business partners.

Other organizations have complained that business associate contracts would be complex and result in significant time and resource burdens, and would require the writing or rewriting of many new contracts. Having contracts in place specifying what agents are permitted to do with sensitive health information just makes good business sense. Additionally, the implementation specifications for business associate contracts are clear and straightforward and should not result in complex contracts. In order to reduce any administrative burden, covered entities are free to develop standard contracts or standard addenda to existing contracts.

Sec. 164.504

Most people get their health insurance through employer-sponsored health plans governed by ERISA (the Employee Retirement Income Security Act). Many fear that employers know more than they should about employees' (and dependents') private medical information and may use that information inappropriately to make employment decisions. The final regulation goes as far as it can to protect workers and their dependents from inappropriate disclosures of information generated through health plan operations. However, a great deal of individually identifiable health information available through occupational health programs can still be accessed by employers and human resource departments and used to make decisions relating to hiring, firing and promotional opportunities.

Statutory limitations inherent in HIPAA prevent this rulemaking from fully protecting all health records held by employers. It is imperative that both HHS and Congress recognize that a great deal of health information collected and maintained by employers does not flow from their operation of an employee health plan. Because these gaps in protection exist, employers will continue to have relatively free access to personal health information obtained through fitness-to-work examinations, occupational safety and health initiatives, and workers' compensation programs. The only remedy for this problem is additional federal legislation to cover all health care providers.

For example, many health care providers who are in workplace settings are not considered "covered entities" under the new rules since they do not engage in any of the "standard HIPAA transactions" (submitting claims, billing or transmitting information). Therefore, the employee health information collected by them in the course of their duties is not protected under the final rule. Despite having ethical principles to maintain confidentiality, these providers can be forced to turn over personal health information to management and human resources personnel who have hiring, firing and promotion capacity.

Additionally, information sent from an employee's primary care provider to a health care provider in a workplace setting may also be unprotected. If an employee is being treated by her primary care provider for breast cancer, a release and consent is legally required for her provider to send health information to the employer about the employee's "return to work" restrictions. Information released for payment of health claims for treatment or surgery would be protected under the HHS rules. However, once received by the health care provider responsible for the employer's productivity management and return to work programs, that information loses its protection if the receiving health care provider does not engage in "standard HIPAA transactions."

Again, legislation establishing a comprehensive federal health information privacy law is necessary to be able to reach all medical records regardless of the medium in which they are created and/or maintained and regardless of who holds the records. AAOHN also believes the comprehensive health privacy legislation should provide protections against inappropriate uses and re-disclosures after an authorized release.

In light of the limitations which flow from the narrow scope of the HIPAA statute, AAOHN very much supports provisions that require the erection of firewalls to separate the group health plan functions of the employer/plan sponsor from the rest of the employer/plan sponsor. Firewalls are essential whether employees of the plan sponsor perform only functions related to the administration of the group health plan or combine those responsibilities with other job functions. These safeguards are essential to protect privacy given HIPAA's failure to allow HHS to reach employers/plan sponsors directly and the genuine concerns of the public about access to personal health information by employers. AAOHN only wishes that Congress would expand the authorizing legislation to permit the creation of similar firewalls around records held in occupational health departments manned by health care providers who do not engage in HIPAA standard electronic transactions.

Sec. 164.512 and Sec. 164.514

AAOHN believes there are a number of other weaknesses in the final regulation, most especially the regulation's treatment of law enforcement access and marketing and fundraising by covered entities, but even these serious weaknesses do not warrant further delay in the effective date. Nor, despite the importance of these issues to consumers, do we seek to reopen the rule-making process in the hope of achieving changes in these areas.