AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 108–256

HIPAA MEDICAL PRIVACY AND TRANSITION RULES: OVERKILL OR OVERDUE?

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

WASHINGTON, DC

SEPTEMBER 23, 2003

Serial No. 108–23

Printed for the use of the Special Committee on Aging

U.S. GOVERNMENT PRINTING OFFICE

91–119 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SPECIAL COMMITTEE ON AGING

LARRY CRAIG, Idaho, *Chairman*

RICHARD SHELBY, Alabama
SUSAN COLLINS, Maine
MIKE ENZI, Wyoming
GORDON SMITH, Oregon
JAMES M. TALENT, Missouri
PETER G. FITZGERALD, Illinois
ORRIN G. HATCH, Utah
ELIZABETH DOLE, North Carolina
TED STEVENS, Alaska
RICK SANTORUM, Pennsylvania

JOHN B. BREAUX, Louisiana, *Ranking Member*
HARRY REID, Nevada
HERB KOHL, Wisconsin
JAMES M. JEFFORDS, Vermont
RUSSELL D. FEINGOLD, Wisconsin
RON WYDEN, Oregon
BLANCHE L. LINCOLN, Arkansas
EVAN BAYH, Indiana
THOMAS R. CARPER, Delaware
DEBBIE STABENOW, Michigan

LUPE WISSEL, *Staff Director*
MICHELLE EASTON, *Ranking Member Staff Director*

CONTENTS

	Page
Statement of Senator Larry E. Craig	1

PANEL I

Richard Campanelli, Director, Office for Civil Rights, U.S. Department of Health and Human Services	3
Jared Adair, Director, Office of HIPAA Standards, Centers for Medicare and Medicaid Services	22

PANEL II

Cathy Treadway, Medical Practice Administrator, The Woman's Clinic, Boise, ID	53
Mary R. Grealy, President, The Healthcare Leadership Council	65
Alissa Fox, Executive Director of Policy, Blue Cross Blue Shield Association	76
Janlori Goldman, Director, the Health Privacy Project	95

APPENDIX

Questions from Senator Lincoln to HHS	127
Statement of the American Psychiatric Association	129
The Center for Medicare and Medicaid Frequently Asked Questions	132
Additional information submitted by the American Psychiatric Association	134
Statement of the American Clinical Laboratory Association	168

HIPAA MEDICAL PRIVACY AND TRANSITION RULES: OVERKILL OR OVERDUE?

TUESDAY, SEPTEMBER 23, 2003

U.S. SENATE,
SPECIAL COMMITTEE ON AGING,
Washington, DC.

The committee met, pursuant to notice, at 9:34 a.m., in room SD–628, Dirksen Senate Office Building, Hon. Larry Craig (chairman of the committee) presiding.

Present: Senators Craig and Fitzgerald.

OPENING STATEMENT OF SENATOR LARRY CRAIG, CHAIRMAN

The CHAIRMAN. Good morning everyone. Thank you all for being here. I think some of our witnesses, and probably some who would wish to attend, are still struggling in the aftermath of Isabel. With the transportation and traffic lights and, of course, last night's heavy rainstorm, it has slowed everything down a bit. Some of my colleagues will be joining me this morning. It is a busy morning here on the Hill.

We want to thank you all for joining us today. Today's hearing will examine an issue of critical importance to the U.S. health care system and to the 40 million seniors who depend upon it.

Seven years ago, Congress enacted the Health Insurance Portability and Accountability Act, otherwise known as HIPAA. At that time, HIPAA's insurance coverage provisions were the pieces that received the lion's share of the attention, and few paid much attention to other but equally significant health care changes buried within the bill.

Today, 7 years later, two such provisions are at long last emerging from a long and tortuous regulatory process. One of these, a new set of requirements governing medical information privacy, went into effect in April. The other is a bundle of new regulations for standardizing medical claims and transactions which is scheduled to go into effect just three short weeks from now.

Few can argue with the underlying intent of these regulations, namely, the streamlining of health care transactions and the protection of medical privacy. However, as is often the case with Federal rulemaking, a kernel of congressional intent has grown into a towering tree of regulatory complexity that I don't think even Isabel could have blown over this past week.

But even with the Federal bureaucracy standards, HIPAA is extraordinary. The privacy provisions in the original law, for example, numbered just 337 words, whereas the final HHS regulation now runs up to 101,000 words. I have heard from many Idaho doc-

tors, patients and others, who are deeply troubled by the confusion, disruption and uncertainty these new rules are creating in the health care system.

During the month of August, and for the last couple of years, at the town meetings that I regularly hold in my State, doctors and providers attended expressing great frustration over what is anticipated. More onerously, the looming HIPAA transaction rules, if they are not reasonably implemented by CMS, threaten to trigger what some say may be a train wreck of stopping payments, cash-flow disruptions, denied care, or even a widespread revision from electronic back to paper claims, precisely the opposite effect Congress intended.

Legislation I sponsored in the last Congress postponed the implementation of the transaction rules by one year, but it is clear that grave problems remain. Meanwhile, the new HIPAA Privacy Rules are continuing to cause confusion among patients, providers and insurers. Stories of hospitals turning away family members seeking information about their loved ones, as well as ideological and disruptive effects, are common among the letters I receive from my constituents.

Also disheartening is the fact that these new regulations are costing doctors, hospitals, health plans and, inevitably, patients, millions if not billions in compliance costs. We would be remiss if we failed to ask: are the benefits from these new regulations worth the heavy bite they are taking out of our country's already squeezed health care budgets? Are needed resources being diverted from the quality of patient care, and equally important, is HHS doing everything it can to implement a smooth and reasonable process?

Here today are senior officials from HHS to answer some of these questions, as are representatives of providers, insurers, and patients respectively. So I look forward to their testimony.

On our first panel today we will hear from the officials at HHS most directly responsible for overseeing both the new transaction regulations and the recent medical privacy rules.

Jared Adair is Director of HIPAA Standards for the Center for Medicare and Medicaid Services, the agency charged with implementation and enforcement of the codes and transactions.

Also with us is Rick Campanelli, Director of the Office of Civil Rights at HHS, the office charged with a similar role, managing HIPAA's medical information privacy requirements.

Miss Adair, we are eagerly interested in hearing from you about CMS's plans for the looming October 16 implementation deadline. As you know, with only weeks to spare, providers, payers and others are waiting with baited breath for the directions from CMS, and I'm hopeful that you can clarify for us today your agency's intentions as specifically and clearly as possible.

Also, Director Campanelli, we are looking to you to provide us with a much-needed clarification about what the new Privacy Rules or do not do, or do not require, in common practice situations and about what your agency is doing to make continuing implementation as smooth as possible. Confusion, as you know, runs very, very high amongst all those that I have mentioned.

So, with that, Director Campanelli, why don't we start with your testimony this morning, and then we will turn to Miss Adair. Thank you both for being with us.

STATEMENT OF RICHARD CAMPANELLI, DIRECTOR, OFFICE FOR CIVIL RIGHTS, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. CAMPANELLI. Thank you, Chairman Craig. I appreciate the opportunity to appear before you today to discuss the HIPAA Privacy Rule. As Director of the HHS Office for Civil Rights, I oversee, as you said, "The office that has responsibility for implementing, enforcing and aiding covered entities to come into compliance with the rule."

Just over a year ago, on August 14, 2002, Secretary Thompson finalized modifications to the Privacy Rule that strengthened its privacy protections and improved workability. With the rule's effective date last April, patients now have critical Federal protections over the privacy of their medical records, rights to access and to correct errors in their medical records, rights to control how their protected health information is used and disclosed, and a clear avenue of recourse if the rights afforded by the rule are violated.

I know that some 5 months now after the compliance date has passed that the committee is interested in hearing how compliance is proceeding and what the Department is doing to promote compliance and to address areas of confusion that may have arisen with respect to the rule. A number of the concerns that have come to our attention actually are not a problem with the rule itself but, rather, misconceptions about the rule, and we are working hard to correct those misconceptions, as you will hear.

For instance, along the lines of some of those misconceptions, we have seen reports that doctors may not share patient information with other providers unless they first have a patient's expressed written consent to do so. That's not true, or perhaps it's more accurate to say that we fixed that a year ago. The August, 2002 Privacy Rule modifications specifically allowed doctors and other providers to share this information for treatment purposes, to obtain payment, or to carry out their day-to-day operations without first having to obtain a patient's written approval.

Along with having made that and other essential modifications before the rule went into effect, we have worked hard to provide extensive technical assistance to covered entities to help them comply with the rule and to minimize the cost and administrative burden of compliance. For example, we issued extensive guidance and answers to frequently asked questions so that entities have ready and free access to correct information. We must be doing something right, because our data base, with some 200 frequently asked questions that are searchable, has been accessed over 1.2 million times since the beginning of the year, most of that just in the last few months.

If you look at Exhibit 2 in your materials and also up here, the second chart on the wall, the sample that you will see shows just the first opening page of those FAQs, and it shows that these FAQs set the record straight and clarify misconceptions on a wide range of issues.

While it is still early to assess compliance with the rule overall, we believe that, as a result of our modifications and technical assistance, covered entities are widely complying with the rule, individuals are widely benefiting from the important privacy protections they received, and misconceptions are being resolved and eliminated.

We recognize and are sensitive to the costs necessarily associated with the implementation of the rule. That concern was behind the modifications which improved workability and reduced compliance costs. In December, 2000, we estimated costs associated with the rule, as restated in my testimony, and have seen cost estimates from time to time from various industry sectors, but we can't evaluate how credible those industry reports are. We note that most of the industry estimates we saw arose prior to the rule's implementation, and many times were associated with dire predictions of collapse of the entire health care system, which obviously wasn't correct.

Nevertheless, we remain attuned to the wide range of industry and consumer groups who inform us about their perspectives on the impact of the rule, often within particular industry segments. In addition, we are continuing to develop and publish guidance to assist covered entities in complying with the rule. Let me highlight some particular elements of that guidance.

We have reached tens of thousands of people through our presentations on the Privacy Rule over the last couple of years. With a toll-free line we sponsor together with CMS, we received 14,000 phone calls just since April 1, and we responded to those calls. It's an indication, we hope and expect, of success in this regard, in that the volume of calls we are receiving now is about a third of what it was when the rule first went into effect in April.

It is gratifying that many of the questions we get on those calls and otherwise can be readily answered from the material on our website. I won't go through all of them, but if you look at Exhibit 1 there, that is the opening page of our website. There are some important documents there that are helpful to doctors and small providers like the ones you have reflected on. For example, there is a summary of the Privacy Rule, which is a clear summary, you can click through to particular documents that give you FAQs on particular topics, a covered entity decision tool, and sample business associate contract provisions. We even have a segment of the website that is focused on small providers where we have information that we think is relevant to folks that you mentioned you are concerned about.

Finally, two other points. We also appreciate the assistance of other groups, including members of your second panel today, such as the Healthcare Leadership Council and the Health Privacy Project, which have produced important information about the rule. We have met with each of those groups and many others.

Our commitment to help covered entities comply with the rule continues even as we are now pursuing our enforcement responsibilities, and in that process, Congress mandated in HIPAA that the Department resolve complaints through informal resolution with covered entities. The Privacy Rule similarly calls upon OCR to provide technical assistance to covered entities in appropriate

circumstances, even in the context of resolving a complaint. Our approach to compliance and enforcement is to employ a variety of enforcement options available to us, as needed, to ensure that individuals receive the privacy protections afforded by the rule.

At the same time, our experience to date is consistent with our expectation, that we will be able to resolve most complaints through voluntary compliance and informal resolution, the most expeditious way of effectuating the rights to the privacy of protected health information.

Thank you for the opportunity to make this presentation. I look forward to your questions.

[The prepared statement of Mr. Campanelli follows:]

STATEMENT

BY

Richard Campanelli, Director
Office for Civil Rights
U.S. Department of Health and Human Services

A Hearing Before The
Senate Special Committee on Aging

628 Dirksen
Senate Office Building
9:30 A.M.
September 23, 2003

Chairman Craig, Senator Breaux, distinguished members of the Committee, I welcome the opportunity to appear before you today to discuss the implementation of the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As the Director of the Office for Civil Rights (OCR), within the U.S. Department of Health and Human Services, I oversee the office that has responsibility for implementing, enforcing, and aiding covered entities to come into compliance with the Privacy Rule.

By way of background, Congress enacted HIPAA in 1996, among other things, to improve the efficiency and effectiveness of the health care system, through "administrative simplification" provisions that created a process for the establishment of standards and requirements for the electronic transmission of certain health information.[1] At the same time, Congress recognized that administrative simplification must be accompanied by protections for the privacy and confidentiality of personal health information, since, as a consequence of more efficient transmission of health information, private health information also would become more readily accessible. Therefore, in enacting HIPAA Congress directed that standards be developed to protect the security and privacy of health information,[2] and established civil and criminal penalties for various violations of those standards. Pursuant to Congress' mandate, HHS issued a proposed Privacy Rule in November 1999, received over 50,000 public comments, and published a final Privacy Rule in December of 2000. Because of continuing concern over aspects of the Rule, in February 2001, HHS announced that it would reopen the Rule for comments, and, after receiving thousands of comments, in April 2001 it proposed to issue recommended modifications to avoid the unintended consequences of the Privacy

---

[1]Sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, are known as the Administrative Simplification provisions.

[2]In the HIPAA statute, Congress gave itself a deadline for passing a privacy statute of August 21, 1999. Section 264(c)(1) of HIPAA provides that: "If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by [August 21, 1999], the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than [February 21, 2000]."

Rule and improve its workability. Those proposed modifications were published in April 2002, and received some 11,000 additional comments. Finally, just over a year ago, on August 14, 2002, HHS finalized those modifications to improve workability while maintaining strong privacy protections. As covered entities have known since the Rule took effect, most covered entities were required to comply with the Privacy Rule as of the April 14, 2003, with small health plans having an additional year to comply.

The Privacy Rule establishes the Nation's first-ever comprehensive standards for protecting the privacy of American's personal health records. As of April 14, 2003, patients have sweeping federal protections over the privacy of their medical records, rights to access and to correct errors in their medical records, rights to control how their protected health information is used and disclosed, and a clear avenue of recourse if the rights afforded by the Privacy Rule are violated.

We know that the Committee is particularly interested in our experience, and that of covered entities and consumers, with the Privacy Rule now that some five months have passed since April 14. Particularly, Committee staff have advised that the Committee desires to be apprised of any areas of confusion, or misconception, that have occurred after April 14, and how HHS is addressing those issues. Because a number of areas that have received public attention are significantly addressed by modifications to the rule made last August, I will focus on the nature and impact of these modifications, before turning to HHS efforts to promote understanding of and compliance with the Privacy Rule – and to dispel the misconceptions that have arisen about it.

One area of the Privacy Rule that was modified on August 14, which had been the subject of much public response during the comment period, was the requirement to obtain written consents from patients to use or disclose their protected health information to treat them, obtain payment, or carry out day-to-day operations. Requiring consent in these contexts would have been unnecessarily burdensome on patients and providers, and interfered with timely access to quality care, without improving privacy. It would have meant, for instance, that a doctor would have needed a patient to sign a privacy consent before he could use health information to treat that patient; that a specialist contacted by the patient's doctor would have needed to obtain the patient's consent to read treatment information; and that a pharmacist would have needed the patient's consent to fill a prescription written by the provider.

The Privacy Rule modifications removed the requirement that providers must obtain prior consent to use or disclose a patient's health information for treatment, payment or health care operations purposes. While obtaining such consent is optional, this change assured that providers would have ready access to health information about their patients, and could readily share that information for treatment, for payment, and for health care operations so that timely access to quality health care would not be unduly impeded. At the same time, we strengthened the notice requirement by requiring direct treatment providers to make a good faith effort to obtain the patient's written acknowledgment that they received the notice. This ensures that a patient has the opportunity to consider the provider's privacy practices, both to be better informed of how their information may or may not be disclosed, and to be informed of their rights – which had been a primary goal of the consent requirement. Notably, the Privacy Rule retained the protections that give patients the right to decide whether to authorize uses or disclosures of their information for marketing purposes, or to employers.

Similarly, the modified Privacy Rule clarified that with reasonable safeguards, uses and disclosures that were merely incidental to appropriate Privacy Rule uses and disclosures would not constitute a violation of the Rule. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted by the Rule. The Privacy Rule recognizes that communications necessary for quick, effective and high quality health care might unavoidably lead to overheard communications. Thus, a physician may discuss a patient's condition or treatment regimen in the patient's semi-private room, and a pharmacist may discuss a prescription with a patient over the pharmacy counter, provided that reasonable precautions (such as lowered voices and/or talking apart from others) are employed.

Both of these examples demonstrate how the Privacy Rule, as modified, both protects patient information, but avoids imposing unnecessary impediments to quality health care.

Since April 14, 2003 there has been widespread compliance by health plans, health care clearinghouses, and those providers covered by the Privacy Rule ("Covered Entities"). For example, physicians, hospitals, clinics, pharmacies, health insurance carriers, employer group health

plans and others have distributed Notices, required by the Privacy Rule, that tell consumers about how their health information can and cannot be used and disclosed, and their rights, including :

- the right to inspect and obtain a copy of the individual's protected health information;
- the right to amend or correct protected health information;
- the right to request restrictions on certain uses and disclosures of protected health information;
- the right to receive protected health information through confidential communications;
- the right to receive an accounting of certain disclosures of their protected health information;
- the right to receive a copy of the Notice of Privacy Practices; and
- the right to complain to a covered entity or to OCR if an individual believes a covered entity has breached the Privacy Rule.

Given the extensive scope of the protections established in the Privacy Rule, implementation has gone smoothly, without the disruption of the healthcare system that had been predicted in some quarters. This is due in part to the commitment made by the Office for Civil Rights and the Department to public education, a commitment that continues in various outreach efforts, voluntary compliance initiatives, and even in investigation of complaints. And it is due to the attention health care providers have given to the Rule and their efforts to implement it. As I will explain, OCR has produced a wide variety of guidance and technical assistance that is focused and prioritized as we discern the need for further clarification. These efforts have significantly contributed to reducing confusion and eliminating misconceptions that have been reported in these first months of compliance. In many of these areas, confusion appears to have arisen not because of problems with the Privacy Rule itself, but rather due to misconceptions about it. In addition, it appears that providers and other covered entities are also serving to educate their fellow covered entities where overly restrictive practices were initially being adopted and, incorrectly, blamed on the Privacy Rule.

For example, we have heard reports that some covered entities are reluctant to share health information with other providers, for the purpose of treating their patients, claiming that the Privacy Rule requires that patients execute written consents for these disclosures to occur. Providers who

claim that this practice is mandated by the Privacy Rule are incorrect, and apparently are unaware that the Rule was modified specifically to permit treatment disclosures among providers without the need for patient consent. In fact, the Privacy Rule allows doctors, nurses, hospitals, technicians, and other covered health care providers to use or disclose patient health information, including X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes, without the patient's authorization. This includes sharing a patient's health information to consult with other providers, to treat a different patient, or to refer the patient to other providers.

Similarly, we have seen reports and heard from consumers, as you may have heard from your constituents, that providers cannot share information with family members, loved ones, friends, or others whom are identified by the individual as involved in their care or the payment for their care. Again, rather than foreclosing such communications, the Privacy Rule provides a number of common-sense methods which appropriately permit such disclosures while respecting and protecting an individual's right to control their health information. Under 45 CFR 164.510(b), the Privacy Rule specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care. Where the patient is present and has the capacity to make health care decisions, the covered entity may discuss this information with these individuals if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with these individuals if it can reasonably infer, based on professional judgment, that the patient does not object. For example, if a patient brings a friend to a medical appointment and asks if the friend can come into the treatment room, her doctor can reasonably infer that the patient does not object. Under these circumstances, a doctor or plan can disclose any information that is directly relevant to the family member or friend's involvement with the patient's care, or payment related to the individual's care.

On a related point, this is also the section of the Privacy Rule that allows Congressional staffers to intercede with covered entities on behalf of your constituents who write in and ask your offices to help, for instance, in obtaining treatment, or with a payment question. As I mentioned earlier, where a patient identifies an individual as being involved in their care – as they might when writing to your office and seeking assistance in these matters -- the Privacy Rule permits covered

entities to share information directly related to that involvement in matters pertaining to the constituent's treatment or payment.

We have also heard reports – incorrect, again – that because of the Privacy Rule, hospitals can no longer maintain patient directories so that appropriate information can be provided to family members, loved ones, clergy or other members of the public who call to inquire about patients. Along similar lines, we have seen reports that clergy, in particular, can no longer visit members of their congregations in the hospital, because the Privacy Rule forbids clergy access to any information about hospitalized individuals, or to information about the individual's religious affiliation. Though it does not mandate that hospitals maintain such directories or make such disclosures, the Privacy Rule specifically provides and envisions that the common and helpful practice of maintaining such directories will continue. Consistent with the overall approach of the Rule, it lets individuals choose whether their information should be included in the facility directory, or to opt out. Even where, because of emergency or the individual's incapacity, the patient cannot be given the opportunity to opt out, the Privacy Rule allows the covered entity to determine, based on experience and professional judgment, whether including the information would be in the best interests of the patient. This information – including the patient's name, location in the hospital, and general description of the patient's condition) can be accessed by anyone inquiring about the patient by name.

Clergy similarly can access this information by asking for patients by name, of course; but the Privacy Rule also allows hospitals to include in the facility directory, and to disclose to members of the clergy, the religious affiliation of patients who have opted to provide it; and members of the clergy can obtain this information without having to inquire about specific patients by name. As with disclosures of information in facility directories to other members of the public, the patient (or those with appropriate authority to act on their behalf) will have the opportunity to decide whether they want their information included in the directory, or to opt out. If they elect to have the information included, then their loved ones, clergy, or others who inquire can have access to this information.

The misconceptions discussed here are among the most common we have heard. It appears that confusion on these issues is dissipating, as covered entities and consumers become more familiar

with the Rule's requirements. These problems do not arise because of the Privacy Rule, but rather seem to arise either because providers have elected to take a more restrictive approach than the Privacy Rule requires, or because of a misconception about the requirements of the Privacy Rule. To address this latter concern, OCR has conducted, and is continuing to conduct, an extensive public education effort to produce and disseminate a wide range of guidance about various aspects of the Rule that are of concern to the public and to covered entities. And we are pleased that the information we have disseminated is being well received.

Continuing extensive outreach efforts that we undertook in prior years, OCR senior Privacy experts, from Washington DC and throughout our regions, have made well over a hundred presentations during 2003 alone. These include four national, all-day HIPAA Privacy Rule conferences, attended by some 6000 participants, sponsored in conjunctions with universities and key industry groups, in February and March of this year, at which OCR and other Department experts in the Rule offered in-depth seminars and answered questions on all aspects of the Privacy Rule. In addition, OCR has conducted or participated in numerous telephone audio conferences. In one toll-free call arranged for by the Departments' Centers for Medicare and Medicaid Services and paid for by OCR, an estimated 8500 people participated on over 4000 telephone lines. Moreover, in conjunction with the Centers for Medicare and Medicaid Services (CMS), OCR offers a free call-in line, 1-866-627-7728 for HIPAA questions. If the trained operators are unable to answer the questions directly or by reference to resource materials and our website, they refer the caller to an OCR Privacy Rule specialist. Since April 1, combined phone-line operators and OCR staff have received and responded to some 14,000 calls related to the Privacy Rule. In many cases, we are gratified that the questions being raised are addressed by guidance materials posted on the OCR website, www.hhs.gov/ocr/hipaa. It is noteworthy that, in the first week of compliance, some 1334 calls were received by our HIPAA operators for Privacy related matters. But, perhaps as an indication that covered entities and consumers are becoming more familiar with the Privacy Rule, by the week ending September 13, 2003, the number of calls was down to 480, only about a third of the initial volume.

Our website plays a key role in our outreach activities, and has enabled us to post and broadly disseminate information that provides additional clarification in helpful areas, and to

clear up misconceptions when they arise. In turn, providers can use these posted materials to educate other providers who, for instance, believe that they cannot share treatment information with each other, without patient consent; it is also useful to patients and their loved ones who seek to correct the misconceptions of hospitals or other providers who mistakenly fail to grasp the latitude afforded by the Privacy Rule to share information with loved ones. From January through July 2003, OCR's Privacy Rule homepage received 847,800 visits.

We want to focus on the information available at this website since it offers a myriad of helpful information for consumers, and technical assistance for covered entities. [See Exhibit 1.] For instance, it includes:

- a comprehensive *Summary of the HIPAA Privacy Rule*, which is linked to other guidance on specific topics referenced in the *Summary*. It is an excellent means of obtaining a clear overview of the Privacy Rule, and finding more thorough information on particular topics;
- A *Covered Entity Decision Tool*, an interactive tool that provides extensive information to assist entities in determining whether they are covered by HIPAA
- Sample *Business Associate Contract Provisions*,
- extensive guidance on particular aspects of the Rule, including
  - General Overview
  - Incidental Uses and Disclosures
  - Minimum Necessary
  - Personal Representatives
  - Business Associates
  - Uses and Disclosures for Treatment, Payment and Health Care Operations
  - Marketing
  - Public Health
  - Research
  - Worker's Compensation Laws
  - Notice
  - Government Access

- the HHS National Institute of Health's Guide to Research, "*Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*", with related information for Institutional Review Boards, and about Authorizations for research;
- the HHS National Institute of Health's Guide to Research, *"Authorizations for Research and Institutional Review Boards"*
- the Center for Disease Control's Guidance, *"HIPAA Privacy Rule and Public Health"*
- a fact sheet for consumers, *"How to File a Health Information Privacy Complaint"*
- a fact sheet for consumers, *"Protecting the Privacy of Patient's Health Information"*

A key feature of our website, accessed over 1.2 million times since January of this year is our database with over 200 searchable Frequently Asked Questions ("FAQs") (EXHIBIT 2). The database is simple to use, and provides clarifications on many different aspects of the Privacy Rule, including some of the areas that we have already discussed. For instance, there are a number of questions that address permissible disclosures for treatment and disclosures to clergy. In addition, we are in the process of posting additional Questions and Answers with guidance on informing visitors about a patient's location in a facility or a patient's general condition; and disclosures to family members.

Our website is also organized to be as helpful as possible. For instance, we include a link focused on materials we believe are of particular interest to small providers and small businesses.

Finally, we are developing additional targeted technical assistance materials, focusing on explaining the Privacy Rule to consumers as well as specific industry groups, required to comply with the Rule such as smaller health care providers, institutional health care providers, health plans, group health plans, health care clearinghouses, and state and local governments .

We are pleased that the industry has developed a better understanding of the Rule, in large part because of the workability changes we adopted last year, and the extensive guidance and FAQs we have published.

I also want to discuss our experience enforcing the Rule and the Department's enforcement posture. OCR has the authority to investigate complaints and it has authority to conduct reviews of covered entities for compliance with the Privacy Rule. As a practical matter, our efforts are primarily complaint-driven, though we have compliance review authority in case we become aware of a situation where no complaint has been filed, but which demands our attention. Any person can file a complaint with OCR, and in the first five months since the compliance date, we have received over 1800 complaints. We have already been able to resolve and close about 30% of those complaints, either because they did not raise a privacy issue, because the action complained of did not constitute a violation of the Rule, or because we were able to resolve the matter expeditiously and informally – through voluntary compliance – usually after providing some technical assistance.

The Privacy Rule provides that HHS will seek cooperation of covered entities in obtaining compliance and can provide technical assistance to covered entities to help them voluntarily comply with the Rule, even after investigations begin. OCR continues to encourage voluntary compliance from covered entities because it is often the quickest and the most efficient means of ensuring that individuals benefit from the protections in the Rule. Of course, even in instances where OCR is giving technical assistance, the responsibility for compliance remains with the covered entity. In appropriate circumstances Congress has provided that the Department may seek to impose civil penalties under the statute: civil penalties may not be imposed for Privacy Rule violations if the person did not know, and by exercising reasonable diligence would not have known, of the violation; or if failure to comply was due to reasonable cause and not willful neglect, and the entity corrects the violation within thirty days of when it knew or should have known of the error. While OCR continues to seek informal resolution through voluntary compliance wherever appropriate, and expects to be able to resolve the vast majority of cases through these informal means, it will employ the variety of enforcement options available as needed to ensure that consumers receive the privacy protections afforded by the Rule.[3]

---

[3]The Department of Justice is responsible for enforcement of HIPAA violations that are subject to criminal penalties.

Finally, I would like to take a moment to address the costs associated with implementing the Privacy Rule, in which the Committee has expressed an interest. We estimated in the preamble to the December 2000 Rule that the Privacy Rule would produce compliance costs of $17.6 billion (with present value costs of $11.8 billion over ten years- 2003-2012). Subsequently, in adopting the August 2002 modifications, the Department estimated that improvements in workability in the modifications, which helped to avoid unintended consequences of the Privacy Rule, would lower the compliance cost of the Privacy Rule by approximately $100 million over ten years.

We also conducted a Regulatory Flexibility Analysis of the economic impact of the Rule on small entities, i.e., organizations with less than $5 million in annual revenues.[4] We noted in our assessment of the costs associated with compliance that the Privacy Rule is flexible and scalable, i.e., wherever possible, the Rule provides a covered entity with flexibility to create policies and procedures that are best suited to the entity's current practices in order to comply with the Rule's requirements. This approach allows covered entities to develop policies and practices that achieve the goal of protecting the privacy of individually identifiable health information, as set forth in the Rule, in a way that is most efficient for them. HHS adopted this scaled approach to minimize the burden on all entities, with an emphasis on small entities. We estimated in December 2000 that the total costs to small businesses of complying with the final rule in the initial year of 2003 would be $1.9 billion and that the ongoing costs to small business from 2004 to 2012 would be $9.3 billion; and we stated in August 2002 that the impact of the published modifications would be *de minimus* on small entities.[5]

HIPAA states that "[a]ny standard adopted under this part [i.e., all HIPAA administrative simplification provisions, including those related to uniform standards for Transactions and

---

[4]We assumed that small business in the health care sector affected by this Rule could include such businesses as: nonprofit health plans, hospitals, and skilled nursing facilities, small businesses providing health coverage, small physician practices, pharmacies, laboratories, durable medical equipment suppliers, health care clearinghouses, billing companies, and vendors that supply software applications to health care entities.

[5]In addition, in our December 2000 Rule, we estimated that the total federal costs under this Rule would be approximately $196 million in 2003 and $1.8 billion over ten years.

Code Sets] shall be consistent with the objective of reducing the administrative costs of providing and paying for health care." While Congress and the Department recognized and anticipated that implementation of the Privacy Rule would be accompanied by significant costs, as set forth above, it was also anticipated that these costs would be offset by efficiencies realized in other aspects of the Rule. In addition, the Department has sought – through adoption and modification of the Privacy Rule, through its public outreach and technical assistance, and through its approach to compliance – to accomplish two key goals: protecting the privacy of health information, while not erecting barriers that unduly impede access to quality health care.

The Office for Civil Rights and the Department have taken significant steps to help covered entities come into compliance with the Privacy Rule, and we are committed to continuing these efforts. We believe our efforts have contributed significantly to reducing the burden and the costs of compliance, and have helped to clarify misconceptions that have arisen with respect to the Privacy Rule. The Department recognizes, as it always has, that significant costs would be associated with achieving the protections and safeguards called for in the Privacy Rule, but we continue to believe that efficiencies to be realized through Administrative Simplification will outweigh these costs. Even so, the Department and OCR are working diligently to ease these costs through our extensive public outreach and technical assistance efforts, through our emphasis on voluntary compliance efforts in all appropriate circumstances. We believe these efforts are accomplishing the goals highlighted by Secretary Thompson when announcing final modifications to the Privacy Rule a year ago: providing a foundation of federal protection for the privacy of health information, while not impeding access to quality health care.

Thank you for this opportunity to address the committee. I look forward to the opportunity to respond to your questions.

Answers to your Frequently Asked Questions

What's New in Privacy

- New combined regulation text for privacy, security, and enforcement rules, unofficial version [PDF] - 9/12/03
- New FAQ on Notices that apply to multiple states - 9/4/03
- New FAQs on:
  - Accounting for Public Health Access to Records
  - Accounting for Date of Access - 8/28/03
- OCR issues caution about misleading marketing on HIPAA training
- New OCR page targets small providers - 7/21/03
- OCR powerpoint

Office for Civil Rights - HIPAA

Medical Privacy - National Standards to Protect the Privacy of Personal Health Information

For Consumers

- Fact Sheet: Protecting the Privacy of Patients' Health Information
- How to File a Health Information Privacy Complaint | [En Español]

General Background Information

- What is the Privacy Rule and why has HHS issued regulations?
- **Privacy Rule Summary** [PDF] [RTF]

HIPAA Regulations & Standards

- The Privacy Rule
- HIPAA Statute
- The Security Rule
- Transactions and Code Set Standards
- Identifier Standards

Compliance & Enforcement

- How to File a Health Information Privacy Complaint
- Interim final rule: Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings [PDF] [DOC]

How to Contact OCR

Educational Materials

- **Summary of HIPAA Privacy Rule** [PDF] [RTF]
- Fact sheets and Guidance on Specific Aspects of the Privacy Rule
- Am I a Covered Entity?
- Your Frequently Asked Questions on Privacy
- Sample Business Associate contract
- The Privacy Rule and Public Health
- The Privacy Rule and Research
- Misleading Marketing on HIPAA Training
- Full List of Educational Materials

For Small Providers/Small Businesses

HIPAA-Related Links

- Centers for Medicare and Medicaid Services (CMS)
- The Privacy Rule and Public Health (CDC)
- The Privacy Rule and Research (NIH)
- National Committee on Vital and Health Statistics (NCVHS)
- Workgroup for Electronic Data Interchange
- Portability of Health Coverage - _Dept. of Labor
- Full List of HIPAA-Related Links

Questions & Answers

Answers Suggest a Question

Search Browse

Category
Privacy of Health Information/HIPAA
All Sub-Categories

Search Text (optional) Search Tips

Search

197 Answers Found **Page: 1 of 10 Go**

Subject

1 Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?
2 Who must comply with these new HIPAA privacy standards?
3 May health care providers leave messages at patients' homes or mail reminders to their homes?
4 What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule?
5 May health care providers use sign-in sheets or call out names in waiting rooms?
6 Can a physician's office FAX patient medical information to another physician's office?
7 Do business associates have obligations to individuals with respect to their information?
8 Does the HIPAA Privacy Rule allow parents the right to see their children's medical records?
9 Does the HIPAA Privacy Rule require that covered entities document all oral communications?
10 May health care providers place medical charts on exam room doors?
11 What does the HIPAA Privacy Rule do?
12 Is an authorization needed to send a medical record to another provider who is treating the patient?
13 What types of insurance are NOT covered under HIPAA?
14 Under what conditions may a health care provider use, disclose, or request an entire medical record?
15 Must I post my entire notice, or may I just post a brief description of it?
16 May a health care provider disclose parts of a medical record that were created by another provider?
17 Must a health care provider give a copy of its notice to everyone, or just those that ask for it?
18 Is a business associate contract needed for janitorial services and the like?
19 When is a health care provider a business associate of another health care provider?
20 Does the HIPAA Privacy Rule require a business associate to create a notice of privacy practices?

Answer ID
349
Category
Privacy of Health Information/HIPAA Disclosures for Law Enforcement Purposes
Date Updated
03/03/2003 06:35 PM

Will the Privacy Rule make it easier for police and law enforcement to get my medical information?

Question

Will this HIPAA Privacy Rule make it easier for police and law enformcement agencies to get my medical information?

Answer

No. The Rule does not expand current law enforcement access to individually identifiable health information. In fact, it limits access to a greater degree than currently exists, since the Rule establishes new procedures and safeguards that restrict the circumstances under which a covered entity may give such information to law enforcement officers.

For example, the Rule limits the type of information that covered entities may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. Similarly, under most circumstances, the Privacy Rule requires covered entities to obtain permission from persons who have been the victim of domestic violence or abuse before disclosing information about them to law enforcement. In most States, such permission is not required today.

Where State law imposes additional restrictions on disclosure of health information to law enforcement, those State laws continue to apply. This Rule sets a national floor of legal protections; it is not a set of "best practices."

Even in those circumstances when disclosure to law enforcement is permitted by the Rule, the Privacy Rule does not require covered entities to disclose any information. Some other Federal or State law may require a disclosure, and the Privacy Rule does not interfere with the operation of these other laws. However, unless the disclosure is required by some other law, covered entities should use their professional judgment to decide whether to disclose information, reflecting their own policies and ethical principles. In other words, doctors, hospitals, and health plans could continue to follow their own policies to protect privacy in such instances.

The CHAIRMAN. Thank you very much for that presentation.

Now, Miss Adair, we will turn to you. Please proceed.

STATEMENT OF JARED ADAIR, DIRECTOR, OFFICE OF HIPAA STANDARDS, CENTERS FOR MEDICARE AND MEDICAID SERVICES

Ms. ADAIR. Thank you, Chairman Craig, and thank you for inviting me here to discuss the progress that has been made in moving toward compliance with the electronic transaction and code set provisions of HIPAA.

CMS has a dual role in implementing HIPAA. The first is as a regulator and enforcer, and the second is as a covered entity, including Medicare, which is the largest covered entity. CMS also works closely with the State Medicaid programs that are, collectively, the second largest covered entity. From that dual vantage point, I can tell you that substantial progress has been made towards the October 16, 2002 compliance. However, I can also tell you that many entities still have a long way to go until they achieve compliance.

Before I tell you what we have done to avoid unintended consequences on the compliance data, I would like to say that the health care industry continues to believe that the goal of HIPAA standardization is the right goal. What they have found out is that the "devil is in the details" and that accomplishing the goal is harder than originally thought. This is characteristic of many large systems development efforts.

Another characteristic of large systems development efforts is the need for contingency planning. It is critical to acknowledge that things can go wrong and to have contingency plans to mitigate those risks. CMS published enforcement guidance that preserved October 16, 2003 as the compliance date, but also allowed for those working toward compliance to adopt contingency plans. If they make reasonable and diligent efforts to become compliant, CMS will not impose penalties on covered entities that deploy contingencies to ensure the smooth flow of payments.

Specifically, as long as a health plan demonstrates its active outreach and testing efforts, it can continue processing payments to providers, even if providers cannot submit a compliant claim.

While the industry welcomed our guidance, there were many who would have liked us to go farther. They wanted a legal safe harbor, but we went as far as the law permitted us. Accordingly, some health plans and payers are still reticent to announce or deploy contingency plans because of the potential of being viewed as legally noncompliant. To alleviate these concerns, CMS has been urging plans and payers to review the guidance, to assess their training partners' readiness, to consider their good faith efforts, and, as appropriate, to deploy a contingency plan.

For example, Medicare is able to accept and process compliant transactions, but on September 4, CMS announced its contingency plan would be to accept and process transactions that are submitted in a legacy format, while continuing to work with their trading partners toward compliance. Just today, Administrator Tom Scully and Tom Grissom, Director of the CMS's Center for Medicare Management, announced the deployment of the Medicare con-

tingency plan after reviewing statistics showing unacceptably low numbers of compliant claims being submitted. This will ensure the cash-flow to Medicare fee-for-service providers will not be disrupted.

Another factor for consideration is the cost of implementation. The rule's impact analysis estimated a new savings to the health care industry, as a whole, of $30 billion over a 10-year period. The estimates were difficult to make. For example, there was no existing comprehensive base line showing the extent of electronic interchange in the industry, nor which transactions and code sets were in use. Many covered entities have revised upward their cost estimates because they have encountered unexpected complications.

Aware that such a change to industry business processes would be a coster, we looked for ways to minimize the cost. First, we adopted standards that were developed by the industry and already in widespread use. Second, we provided support and education to facilitate implementation. Third, when implementation efforts highlighted potential portions of the standards that would have increased cost, CMS proposed and adopted modifications.

While difficulties exist in achieving compliance, this is not the time to waver in our commitment to offer order and consistency in health care administrative transactions. Rather, this is the time to work with covered entities as they strive for the finish line.

CMS has provided the potential for a smooth transition through our enforcement guidance for those still working to achieve compliance. We expect that plans and payers will favorably consider deploying contingencies to mitigate unintended adverse effects on covered entities' cash-flow and business operations. CMS expects that these contingencies will mitigate unintended consequences of the transition.

We are often asked what will happen on October 16, 2003. Certainly, there will be problems, but plans and payers' willingness to appropriately deploy contingency plans will facilitate a smooth transition. The health care industry's combined emphasis on HIPAA compliance will allow us to make the promises of HIPAA a reality.

Thank you. I look forward to answering your questions.

[The prepared statement of Ms. Adair follows:]

STATEMENT OF

JARED ADAIR

DIRECTOR

OFFICE OF HIPAA STANDARDS

CENTERS FOR MEDICARE & MEDICAID SERVICES

BEFORE THE

SENATE SPECIAL COMMITTEE ON AGING

SEPTEMBER 23, 2003

TESTIMONY OF
JARED ADAIR
DIRECTOR
OFFICE OF HIPAA STANDARDS
CENTERS FOR MEDICARE & MEDICAID SERVICES
ON
HIPAA TRANSACTION AND CODE SET REQUIREMENTS
BEFORE THE
SENATE SPECIAL COMMITTEE ON AGING
SEPTEMBER 23, 2003

Chairman Craig, Senator Breaux, distinguished Committee members, thank you for inviting me to discuss the progress that has been made in moving toward compliance with the electronic transaction and code set provisions of the Heath Insurance Portability and Accountability Act (HIPAA).

The Centers for Medicare & Medicaid Services (CMS) has a dual role in the implementation of HIPAA administrative simplification provisions. In the first role, which is delegated by HHS, CMS acts as a regulator and enforcer of the HIPAA transaction and code set standards. As the Agency responsible for paying Medicare claims, CMS fulfills the second role as a covered entity like thousands of other payers and submitters. Of all the programs that HIPAA covers, Medicare is the largest covered entity. CMS also works with the State Medicaid programs, which collectively are the second largest covered entity. Although there is a firewall between the two distinct roles of the Agency, our regulatory and enforcement activities are improved by our understanding of the operational and implementation issues experienced by a covered entity.

Not long ago, physician offices and hospitals manually produced health care bills and claims and sent them to health care plans for adjudication and payment. As computer technology became prevalent in billing offices, bills and claims were created and submitted electronically for payment. The transition from paper to electronic transactions has produced a number of benefits, including less expensive processing costs

and faster transactions. However, the transition merely moved proprietary forms and code sets from paper to electronic media. It did not bring about real administrative simplification. Billing offices still had to accommodate the computer formats and codes for each health plan that was billed, creating a situation in which billing offices had to keep separate instructions and billing manuals for each and every health plan they billed.

While the health care industry has continued to prepare and submit bills and claims to the specific requirements of each health care payer, time has not stood still for other industries. The banking and shipping industries have advanced from simply using computers to a higher level of utilization that optimizes computer use through standardization to meet the business needs of their mobile and informed customers. For example, because the banking industry has agreed upon transaction standards, customers enjoy the safe use of their bankcards at ATMs around the world. Likewise, standards in the shipping industry make it possible to track and deliver parcels worldwide. Such standards and interoperability will benefit the entire health care industry.

The administrative simplification provisions of HIPAA built on earlier efforts to introduce standardization to the administrative transactions of the health care industry. Instead of relying on plan-specific formats, health plans and payers will now use one format for a claim, remittance advice, or eligibility inquiry. Industry representatives expressed to Congress the need for standards. While there is a general agreement that standards are beneficial, it is fair to say that questions arise on the specifics of the standards. In addition, standard code sets will be used within those formats. As a result, the format and codes will be consistent or standardized regardless of which health plan received a claim.

STANDARDIZING TRANSACTIONS AND CODE SETS

There are several factors involved in standardizing a transaction. Parties must agree on the pieces of information – the data content – that will be exchanged. This includes information such as "patient name," "address," and amount billed. How each piece of data will be represented – or coded – also requires standardization. Codes have been

developed in the health care industry to represent procedures, diagnoses, the place of service, and other items. There also must be agreement on how to format the data elements and codes for a transaction so that the sender knows how to assemble a transaction and the receiver knows how to interpret it.

As HIPAA intended, the Department of Health and Human Services worked closely with industry standard setting organizations to assess potential candidate standards for the administrative transactions and code sets specified in the law. The transactions encompass many of the "back office" functions of a health care provider, such as claim submission, eligibility queries, claim status queries, and the remittance advice that allows the provider to post insurance payments to patient accounts.

The code sets are clinical codes—covering both diagnoses and procedures--that are used in those transactions. Under HIPAA, a code set is any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis codes, or medical procedure codes. Medical data code sets used in the health care industry include coding systems for diseases, impairments, causes of injury, as well as actions taken to prevent diseases, injuries, and impairments and to diagnose or treat patients. Code sets also are utilized for any substances, equipment, supplies, or other items used by the health care industry. HIPAA requires code sets for medical data in the administrative and financial health care transaction standards for diagnoses, procedures, and drugs. A list of the transactions and code sets is being provided to the committee as a supplement to this testimony.

The transaction and code set standards were adopted by Final Rule issued by HHS in August 2000, with an original compliance deadline of October 16, 2002. The impact analysis contained in that rule estimated a net savings to the health care industry as a whole of $30 billion over ten years. The estimates were difficult. For example, there was no existing baseline showing the degree to which electronic data interchange was in use throughout the healthcare industry, or to assess the extent to which various transactions and code sets were used. Many covered entities, including Medicare, have

revised upward their HIPAA cost estimates because they have encountered unexpected complications during the assessment and implementation process.

However, it is clear that HIPAA is going to improve the administrative costs for everyone in the long term. For example, HIPAA is expected to create significant savings for the health care industry - and the taxpayer - over the first ten years of implementation. It also is important to note that HIPAA carries significant cost-reduction capabilities over time, when taking into account the start-up costs currently being incurred. Health care providers will be able to submit bills in the same format to all payers and be assured the bills will be accepted. Providers also will have the capability to query claim status and eligibility by computer rather than over the phone. Plans will not have to keep or store paper claims. This will reduce overhead as well as improve turnaround time for transactions, both of which should have a positive impact on cash flow.

LOOKING TO INDUSTRY

When CMS began the process to propose and adopt standards, attempts were made to minimize costs to health care entities. Rather than develop new standards, CMS worked with private industry and adopted industry consensus-developed standards as directed by HIPAA. This assured the widest possible participation from those in the industry who understood business needs. Also, efforts were made to adopt standards already in widespread voluntarily use, minimizing the number of entities needing to convert to the standards. The Agency also provided support and education to facilitate implementation. For example, HIPAA implementation guides are available without charge via the Internet. In addition, when initial implementation efforts highlighted some potential problems with the standards that would have increased costs, CMS proposed and adopted modifications. These modifications were published in February 2003 and covered entities are required to comply with the modifications by October 16, 2003.

During the implementation process, industry readiness issues were brought to Congress' attention; and, in response, Congress enacted the Administrative Simplification Compliance Act in December 2001. This allowed non-compliant covered entities to

request a one-year extension to work toward compliance. As a part of the extension request, the entity was required to share its plan of action for achieving HIPAA compliance. Many entities requested extensions, and tremendous progress has been made toward compliance.

HIPAA OUTREACH EFFORTS

Recognizing the state of industry readiness was low and that part of the problem was a lack of awareness, CMS conducted a national outreach campaign about HIPAA's electronic transaction and code set standards. The Agency has employed a multi-faceted approach to reach its diverse target audiences. For example, CMS manages a Website that provides materials designed to help providers and other entities. This site includes checklists, frequently asked questions, and other materials. Providers, office managers, vendors and others also have the ability to e-mail questions to CMS and receive a personal response. CMS has addressed thousands of HIPAA questions already through this system. In addition, CMS has produced and distributed HIPAA videos on VHS cassettes and CDs to hundreds of individual requestors. These videos have broadcast by satellite, on the Internet, and on cable networks across the country.

Our outreach efforts also include provider education conferences, which have been held in all 50 states. To further ensure that information is readily accessible, CMS has worked with many national associations, such as the American Medical Association, the American Hospital Association, the Health Insurance Association of America, and the Blue Cross and Blue Shield Association of America, to share information and participate in forums. CMS also participated in several HIPAA compliance assistance seminars for employers, health plans, and benefits administrators, which have been sponsored by the Department of Labor. Additionally, CMS published a HIPAA public service advertisement in 13 major health care journals and publications.

In an effort to be as accessible as possible, CMS has conducted 12 free national HIPAA Roundtable Conference Calls that have had record-breaking numbers of participants. In addition, many regional Roundtable calls have successfully reached doctors, hospitals,

insurance companies, and others in specific geographic areas. Outreach efforts also include a HIPAA toll-free hotline that provides general information and responses to questions. More than 6,000 calls were handled in August 2003 alone. For those without Internet and e-mail access, a fax-back service to provide HIPAA material is also available. A summary of available resources is attached.

IMPLEMENTATION ISSUES AND PROGRESS

Through the course of working toward HIPAA compliance for the past several years, it has become apparent that the health care industry still agrees standardization is the right goal. However, this goal is more difficult to attain than originally anticipated due to the complexities and volume of health data. As is the case with other endeavors of this size, the "devil is in the details."

With the industry's increased awareness of HIPAA standardization came more issues. These range from the need to collect additional data elements, to the understanding that vendors and software developers could not handle the standardization effort alone. The many relationships that exist between the many providers and the many payers complicate the effort to standardize. In addition, testing before full implementation is an iterative process that takes significant time to ensure success.

Despite the challenges in achieving standardization, the industry has made substantial progress and is moving toward the goal of HIPAA compliance on October 16, 2003. After evaluating the results of testing and the percentage of complaint claims being received and adjudicated in the Medicare and Medicaid environments, reviewing information from provider and payer associations, and surveying information technology research and advisory firms, it has become clear that despite everyone's best efforts, the progress that has been made is not enough to ensure that all health care providers and payers are 100 percent ready to support the uninterrupted continuation of the nation's $1.4 trillion health care payments, a sum that is 14.1% of GDP. Many industry groups share our Agency's concerns.

CONTIGENCY PLANNING

It should be recognized that HIPAA is a significant systems development effort. As such, it is critical to acknowledge that things can go wrong and to have contingency plans in place. As part of its planning and risk management efforts and in response to industry request, CMS developed the attached "Guidance on Compliance" document. This preserved the compliance date as October 16, 2003, but allowed for those working toward compliance to adopt contingency plans.

As noted in the "Guidance on Compliance" document, CMS will focus on obtaining voluntary compliance and use a complaint-driven approach for the enforcement of HIPAA's electronic transactions and code sets provisions. When CMS receives a complaint about a covered entity, that covered entity will have the opportunity to demonstrate compliance, document its good faith efforts to comply with the standards, or to submit a corrective action plan. CMS recognizes that transactions often require the participation of two covered entities and that noncompliance by one covered entity may put the second covered entity in a difficult position. Therefore, during the period immediately following the compliance date, CMS will examine entities' good faith efforts to come into compliance with the standards and will determine, on a case-by-case basis, whether reasonable cause for the noncompliance exists. Pursuant to HIPAA, if CMS finds reasonable cause, the Agency will determine the extent to which the time for resolving the noncompliance should be extended.

CMS will exercise its enforcement discretion, on a case-by-case basis, to not impose penalties on a covered entity that deploys a contingency plan to ensure the smooth flow of payments if it determines that the covered entity is making reasonable and diligent efforts to become compliant and, in the case of health plans or payers, to facilitate the compliance of their trading partners. Specifically, as long as a health plan demonstrates its active outreach and testing efforts, it can continue processing payments to providers. In determining whether a good faith effort has been made, CMS will place a strong emphasis on sustained actions and demonstrable progress toward compliance with the transaction and code set regulations.

While the industry welcomed our guidance, there are those who would have liked additional action. For example, some health plans and payers are still reticent to announce or deploy contingency plans without a legal "safe harbor." CMS believes its guidance and contingency solution goes as far as permissible under the law. To alleviate industry concerns, CMS is urging health plans and payers to review the guidance, assess their trading partners' readiness, consider their "good faith efforts," and, as appropriate, deploy a contingency plan.

For example, while Medicare is able to accept and process HIPAA compliant transactions, CMS is actively assessing the readiness of its own trading partners to make sure that cash flow to Medicare fee-for-service providers will not be disrupted. Recently, CMS shared Medicare's fee-for-service contingency plan with the provider community so that providers could be prepared to work with the Agency should the plan be deployed. Under Medicare's contingency plan, the program will continue to accept and process transactions that are submitted in legacy formats while continuing to work with its trading partners toward compliance with the HIPAA standards. CMS will continue to assess the readiness of its trading partner community, including the number of Medicare submitters who are currently testing and with our contractors, as well as the percentage of complaint claims we are adjudicating. Based on this assessment, CMS will determine whether it will deploy its contingency plan.

As we move toward implementing HIPAA's important standardization requirements, it is critical to examine areas where the health care industry and CMS--both as the regulator and as a covered entity--need to review the implementation process and look for improvements. The industry will review three areas:

1. The use of companion guides that describe situational elements but could be misused to exceed the HIPAA standardization requirements,
2. Required data elements that are not necessarily needed to adjudicate a claim, and
3. Clarification of implementation guidance that is open to interpretation.

CMS, in its regulator role, will consider how the law applies to these matters.

HIPAA is a large and important effort for the health care industry. It will not be easy, but it will be worth all of our efforts. In the end, it will serve as a critical foundation to future improvements to the administrative and electronic systems that support our great health care industry.

CONCLUSION

While difficulties exist in achieving compliance, this is not the time to waver in our commitment to offer order and consistency in health care administrative transactions. Rather, it is the time to work with covered entities as they strive to cross the finish line. CMS has provided the potential for a smooth transition through our enforcement guidance for those who are still working to achieve compliance. The Agency expects that health care plans and payers will consider deploying contingency plans to mitigate unintended adverse effects on covered entities' cash flow and business operations during the transition to the standards. CMS expects these contingency plans will mitigate unintended consequences of the transition on the availability and quality of care.

We are often asked what will happen on October 16, 2003. Certainly there may be problems, but health plans' and payers' willingness to appropriately deploy contingency plans will facilitate a smooth transition. The health care industry's continued emphasis on HIPAA compliance will allow us to make the promises of the HIPAA a reality.

Chairman Craig, Senator Breaux, and Committee members, thank you again for the opportunity to testify. I hope I have expressed the commitment CMS has to the transaction and code sets provisions of the HIPAA statute. I would be pleased to answer any questions you might have.

Guidance on Compliance with HIPAA Transactions and Code Sets
AFTER THE OCTOBER 16, 2003, IMPLEMENTATION DEADLINE

BACKGROUND
To improve the efficiency and effectiveness of the health care system, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which included a series of "administrative simplification" provisions that required the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions. All covered entities must be in compliance with the electronic transactions and code sets standards by October 16, 2003.

The law is clear: October 16, 2003 is the deadline for covered entities to comply with HIPAA's electronic transaction and code sets provisions. After that date, covered entities, including health plans, may not conduct noncompliant transactions. With the October deadline just ahead, HHS has received a number of inquiries expressing concern over the health care industry's state of readiness. In response, the Department believes it is particularly important to outline its approach to enforcement of HIPAA's electronic transactions and code sets provisions. The Department will continue to provide technical assistance and issue guidance on the transactions and code sets provisions and compliance therewith.

ENFORCEMENT APPROACH
The Secretary has made the Centers for Medicare & Medicaid Services (CMS) responsible for enforcing the electronic transactions and code sets provisions of the law.

CMS will focus on obtaining voluntary compliance and use a complaint-driven approach for enforcement of HIPAA's electronic transactions and code sets provisions. When CMS receives a complaint about a covered entity, it will notify the entity in writing that a complaint has been filed. Following notification from CMS, the entity will have the opportunity to 1) demonstrate compliance, 2) document its good faith efforts to comply with the standards, and/or 3) submit a corrective action plan.

Demonstrating Compliance - Covered entities will be given an opportunity to demonstrate to CMS that they submitted compliant transactions.

Good Faith Policy - CMS's approach will utilize the flexibility granted in section 1176(b) of the Social Security Act to consider good faith efforts to comply when assessing individual complaints. Under section 1176(b), HHS may not impose a civil money penalty where the failure to comply is based on reasonable cause and is not due to willful neglect, and the failure to comply is cured with a 30-day period. HHS has the authority under the statute to extend the period within which a covered entity may cure the noncompliance "based on the nature and extent of the failure to comply."

CMS recognizes that transactions often require the participation of two covered entities and that noncompliance by one covered entity may put the second covered entity in a difficult position. Therefore, during the period immediately following the compliance date, CMS intends to look at

both covered entities' good faith efforts to come into compliance with the standards in determining, on a case-by-case basis, whether reasonable cause for the noncompliance exists and, if so, the extent to which the time for curing the noncompliance should be extended.

CMS will not impose penalties on covered entities that deploy contingencies (in order to ensure the smooth flow of payments) if they have made reasonable and diligent efforts to become compliant and, in the case of health plans, to facilitate the compliance of their trading partners. Specifically, as long as a health plan can demonstrate to CMS its active outreach/testing efforts, it can continue processing payments to providers. In determining whether a good faith effort has been made, CMS will place a strong emphasis on sustained actions and demonstrable progress.

Indications of good faith might include, for example, such factors as:

- Increased external testing with trading partners.
- Lack of availability of, or refusal by, the trading partner(s) prior to October 16, 2003 to test the transaction(s) with the covered entity whose compliance is at issue.
- In the case of a health plan, concerted efforts in advance of the October 16, 2003 and continued efforts afterwards to conduct outreach and make testing opportunities available to its provider community.

While there are many examples of complaints that CMS may receive, the following is one example that illustrates how CMS expects the process to work.

> Example: A complaint is filed against an otherwise-compliant health plan that accepts and processes both compliant and non-compliant transactions while working to help its providers achieve compliance.

In this situation, CMS would 1) notify the plan of the complaint, 2) based on the plan's response to the notification, evaluate the plan's efforts to help its noncompliant providers come into compliance, and 3) if it determined that the plan had demonstrated good faith and reasonable cause for its non-compliance, not impose a penalty for the period of time CMS determines is appropriate, based on the nature and extent of the failure to comply.

For example, CMS would examine whether the health plan undertook a course of outreach actions to its trading partners on awareness and testing, with particular focus on the actions that occurred prior to October 16th. Similarly, health care providers should be able to demonstrate that they took actions to become compliant prior to October 16th. If CMS determines that reasonable and diligent efforts have been made, the cure period for noncompliance would be extended at the discretion of the government. Furthermore, CMS will continue to monitor the covered entity to ensure that their sustained efforts bring progress towards compliance. If continued progress is not made, CMS will step up their enforcement efforts towards that covered entity.

Organizations that have exercised good faith efforts to correct problems and implement the changes required to comply with HIPAA should be prepared to document them in the event of a complaint being filed. This flexibility will permit health plans to mitigate unintended adverse effects on covered entities' cash flow and business operations during the transition to the standards, as well as on the availability and quality of patient care.

Corrective Action Plan (CAP) – After October 16, 2003, in addition to possible fines and penalties imposed, CMS will expect non-compliant covered entities to submit plans to achieve compliance in a manner and time acceptable to the Secretary. More detailed information on CAPs will be forthcoming.

WORKING TOWARD COMPLIANCE

In the few remaining months before the October 16th deadline, HHS encourages health plans and providers to intensify their efforts toward achieving transaction and code set compliance. In addition, HHS encourages health plans to assess the readiness of their provider communities to determine the need to implement contingency plans to maintain the flow of payments while continuing to work toward compliance. Although transaction and code set compliance is a huge undertaking, the result will be greatly enhanced electronic communication throughout the health care community. Successful implementation will require the attention and cooperation of all health plans and clearinghouses, and of all providers that conduct electronic transactions. There is considerable industry support for transaction and code sets, and we all look forward to realizing the many advantages of its successful implementation.

HIPAA Transactions and Code Sets

HIPAA Transactions:

Transaction	Standard
Claims or equivalent encounter information	X12N 837 and NCPDP
Payment and remittance advice	X12N 835
Claim status inquiry and response	X12N 276/277
Eligibility inquiry and response	X12N 270/271
Referral certification and authorization inquiry and response	X12N 278
Enrollment and disenrollment in a health plan	X12N 834
Health plan premium payments	X12N 820
Coordination of benefits	X12N 837
Claims attachments	*PENDING*
First report of injury	*PENDING*

HIPAA Code Sets:

Type	Code Set
Physician services/ other health services	combination of HCPCS and CPT-4
Medical supplies, orthotics, and DME	HCPCS
Diagnosis codes	ICD-9-CM, Vols 1&2
Inpatient hospital procedures	ICD-9-CM, Vol 3
Dental services	Code on dental procedures and nomenclature (CDT)
Drugs/biologics	NDC for retail pharmacy

CMS HIPAA

Electronic Transactions & Code Set

Moving Towards Compliance
September, 2003

Avoid Disruptions in your Cash Flow.....
Have you prepared a contingency plan? If not, consider doing so now so as to avoid any possible disruptions in cash flow. And, contact your payers to test your HIPAA transactions. Less than a month remains until the compliance date of 10/16/03!

New HIPAA Resources!

CMS' Southern Consortium's Achieving Compliance Together (ACT) Team has developed a series of HIPAA presentations that can be viewed via your own computer at your own pace for FREE. The webcast presentations come complete with downloadable slides and other tools. To access these presentations, simply click on the following link:

http://www.eventstreams.com/cms/tm_001/

You can choose any of the following presentations:

1) Message to Providers
2) HIPAA Basics
3) Provider Steps to Getting Paid
4) HIPAA Security
5) CMS Enforcement of T&CS **NEW**
6) 837 for Professional Claims **NEW**
7) 837 for Institutional Claims (Coming Soon)

HIPAA Roundtable!

- **September 25, 2003**
- **2:00 – 3:30** PM EST
- Call in number is **1-877-381-6315**
- Conference ID # is **1596442**

FREE Tools

- **www.cms.hhs.gov/hipaa/hipaa2**
- Call us at **866-282-0659**
- E-mail us at **askhipaa@cms.hhs.gov**

Now Available!

CMS' HIPAA 101 **Video** and **CD-ROM** are packed with tips for preparing your office for HIPAA. Order yours now for only $13.00 at www.NTIS.gov.

Preparing for Compliance with October 16, 2003

CMS is committed to helping you prepare for compliance with the October 16, 2003 HIPAA Electronic Transactions and Code Sets Deadline. We have numerous tools available on our website (see above box) which can be accessed for free, including answers to your frequently asked questions, educational materials, latest news, roundtable transcripts, fax back, and links to regulations. If you need further assistance we have a toll-free hotline in place and an e-mail address where you can seek technical assistance.

HIPAA RESOURCES

9/5/03

CMS Resources

Resources on CMS Website

- **Website** – **http://www.cms.hhs.gov/hipaa/hipaa2/** - Answers to Frequently Asked Questions, links to other HIPAA sites, and information on the law, regulations, and enforcement are located here.
- ***New!* Electronic Submission of Medicare Claims Interim Final Rule** - The Interim Final Rule for Electronic Submission of Medicare Claims was published in the Federal Register on August 15, 2003. This interim final rule implements the statutory requirement found in the Administrative Simplification Compliance Act (ASCA). ASCA requires all claims (with some limited exceptions) sent to the Medicare Program be submitted electronically starting October 16, 2003. The Rule can be accessed at: **http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-20955.pdf**
- **CMS Guidance on Compliance with HIPAA Transactions and Code Sets** – This brief document outlines CMS' approach to enforcement of HIPAA's electronic transactions and code sets on and after 10/16/03. This document can be found at: **http://www.cms.hhs.gov/hipaa/hipaa2/guidance-final.pdf**
- **List of Questions to ask your Vendor** – Use this list to help you understand what questions you should be asking your vendors, clearinghouses, or third party billers to help ensure your transactions are conducted according to HIPAA standards on or after October 16, 2003. Visit the following link to download the list for free: **http://www.cms.hhs.gov/hipaa/hipaa2/Questionsforproviderstoaskvendors.pdf**
- **FREE HIPAA Information Series for Providers** – This series of ten short papers gets straight to the point describing HIPAA and what it means to providers and what is needed to prepare for the electronic transactions and code sets requirements for October 16, 2003. Available on the website in English and Spanish at **http://www.cms.hhs.gov/hipaa/hipaa2/education/infoseri/**
- **FREE Listserves** – Both listserves are operated by the U.S. Department of Health & Human Services
  - **Regulations - http://www.cms.hhs.gov/hipaa/hipaa2/regulations/lsnotify.asp -** Sign up to receive notification when proposed or final rules on HIPAA have been published in the Federal Register (The Federal Register is the place where the government, upon passing a law, tells the public how the law will be implemented).
  - **Outreach – http://list.nih.gov/archives/hipaa-outreach-l.html -** Sign up here to receive free notices on HIPAA announcements, new tools and educational material, and related information.
- **Video** – Now Available! CMS' HIPAA 101 Video and CD-ROM are packed with tips for preparing your office for HIPAA. Order yours now for only $13 at **www.NTIS.gov** (search under "HIPAA" and it is the first item that comes up).
- **Medicare free / low cost billing software** – **http://cms.hhs.gov/providers/edi/** - If you bill Medicare, there is software available to you free or for a small charge. This software is designed only for Medicare claims. Check the above link for the appropriate contact in your state for more information.
- **CMS Medicaid HIPAA web address** - **http://www.cms.hhs.gov/medicaid/hipaa/adminsim/**

HIPAA RESOURCES

9/5/03

Upcoming CMS HIPAA Events

- **FREE HIPAA Roundtable Conference Call** - A good source of information and a forum to get answers to your questions on HIPAA Administrative Simplification. Next call is scheduled for **September 25, 2003** from **2 - 3:30 ET.** Call in number is **1-877-381-6315** and **conference ID = 1596442.**
- **FREE HIPAA Workshop** - September 10, 2003 – Poplar Bluff, MO. Registration preference given to MO providers. RSVP to HIPAAKC@cms.hhs.gov or by calling Uvonda Meinholdt at: 816-426-5783.

FREE CMS Webcast Training

CMS' Southern Consortium has developed a series of HIPAA presentations. Visit the below site to get started. Easy to access at your own computer and at your own pace!
http://www.eventstreams.com/cms/tm_001/

No Internet Access? No Problem.

Looking for information on HIPAA but don't have Internet access? Our **FREE fax back service** is a great way to get around that. Several documents are available by calling **800-874-5894**. Be sure to have your fax number ready when you call.

Contacts for CMS

- **CMS E-Mail box – askhipaa@cms.hhs.gov.** Send HIPAA administrative simplification questions here.
- **CMS HIPAA Hotline –1-866-282-0659** –This hotline has been established to help answer your HIPAA administrative simplification questions

Other HIPAA Resources Outside CMS

- ***Privacy*** – The U.S. Department of Health & Human Services' Office for Civil Rights (OCR) oversees privacy standards.
  - **Visit OCR Website - http://www.hhs.gov/ocr/hipaa/**
  - **OCR Hotline - 1-866-627-7748**

- ***WEDI SNIP*** - WEDI, the Workgroup for Electronic Data Interchange, is an organization working to foster widespread support for the adoption of electronic commerce within healthcare and SNIP is a collaborative healthcare industry-wide process resulting in the implementation of standards and furthering the development and implementation of future standards. This website contains various resources on HIPAA administrative simplification. Visit **http://www.wedi.org/snip/** for more information.
  - Find out if your state has a local WEDI SNIP affiliate – Go to **http://www.wedi.org/snip/public/articles/index%7E8.htm**
  - A resource for information on health plan electronic transaction changes – Go to **http://www.wedi.org/snip/CAQHIMPTOOLS/**

- ***HIPAA Toolkit*** – *HIPAA Transactions and Code Sets Toolkit commissioned by Blue Cross Blue Shield Association.*
  - **http://news.bcbs.com/relatives/20625.pdf**

The CHAIRMAN. Miss Adair, thank you very much for your testimony.

Let me start with questions to you first this morning, because I think you made some very important comments about CMS' plans for implementation on October 16, comments that I expect will be viewed with tremendous interest by thousands of doctors and hospitals and health plans and patients. Because of what you have just said and its importance, let me press you for a few moments for some clarification.

Are you saying that CMS is today announcing a decision to deploy a contingency plan under which Medicare will continue to accept and pay non-HIPAA compliant or so-called legacy claims past the October 16 deadline, at least for a limited period of time?

Ms. ADAIR. Yes, sir. I am indicating that today Administrator Scully did announce that we were deploying the contingency that will allow us to accept, to continue to accept—which we do right now—compliant transactions as well as transactions as we took them prior to HIPAA.

We will continue to monitor. We will continue our good faith efforts of outreach and testing to try to move the rest of the folks from noncompliance into compliance. We will evaluate their progress and then determine how long to keep this contingency in place.

The CHAIRMAN. Well, that's obviously very significant.

Will private, non-Medicare health plans also be directed by CMS to adopt similar contingency plans involving acceptance of legacy claims past the deadline?

Ms. ADAIR. Since we put out our guidance on July 24, we have had meetings with private insurers and talked to them about and encouraged them to do that.

Those decisions are their own business decisions to make. We are not in a position to mandate that they do it, but we have talked to them about the potentials and encouraged them to announce contingencies and, as necessary, to deploy those contingencies.

The CHAIRMAN. Will there be any adverse enforcement consequences to a plan if a private health plan takes this route?

Ms. ADAIR. Should we receive a complaint, sir, that somebody had done that, we would go back to that health insurer and ask them what their good faith effort had been; had they done outreach, had they done testing. If they have, in fact, exercised what we would call good faith effort, there would not be any penalty taken against them for having deployed that contingency.

The CHAIRMAN. Would good faith effort be determined by that kind of analysis?

Ms. ADAIR. Yes, sir.

The CHAIRMAN. When exactly will the details and fine print of CMS' contingency plan be available?

Ms. ADAIR. We will today be sending instructions to our Medicare contractors, so it would be available at that time, sir.

The CHAIRMAN. OK. We're 3 weeks away.

Ms. ADAIR. That is the exact reason, sir, that on September 4, we indicated to providers and to insurance companies, if we were going to deploy our contingency, what it would be, so that they would have an understanding and be able to get themselves ready

for that. We feel like announcing it in advance helps people understand what we would be doing.

The CHAIRMAN. How closely will the actual contingency plan resemble the draft contingency plan informally circulated by CMS in recent weeks?

Ms. ADAIR. Since September 4, sir?

The CHAIRMAN. Yes.

Ms. ADAIR. It will be exactly the same. Our decision today was to deploy that plan.

The CHAIRMAN. Under CMS' contingency plan, for how long past the deadline will Medicare continue to accept legacy claims?

Ms. ADAIR. I cannot give you a specific date, sir. We will be monitoring the percentages of compliant claims in production as well as of our providers who are submitting, and make the decision based upon that as opposed to a date certain.

The CHAIRMAN. Will the contingency plan include not only provisions for payment of noncompliant claims but also protection from adverse enforcement actions?

Ms. ADAIR. Could you ask that one more time? I'm sorry.

The CHAIRMAN. Yes. Will the contingency plan include not only provisions for payment of noncompliant claims but also protection from adverse protection actions?

Ms. ADAIR. I believe—I want to make sure I'm answering the correct question, sir. So the question is, not only are you concerned that not a negative action be taken against the plan, but about providers submitting those claims——

The CHAIRMAN. Yes.

Ms. ADAIR. Should we receive a complaint about one of those providers, we would, in fact, ask them if they had made themselves good faith efforts to try to become complaint. If they had not, we would ask them for a corrective action plan to indicate how they would be moving forward. If they did either of those, either the good faith or corrective action, we would not have any conversations with them about enforcement action.

The CHAIRMAN. OK.

Ms. ADAIR. We would not ourselves—I'm sorry.

The CHAIRMAN. Go ahead.

Ms. ADAIR. We would not ourselves file a complaint against them.

The CHAIRMAN. What is the HIPAA readiness of State Medicaid programs?

Ms. ADAIR. The Medicaid programs, sir, run the gamut. There are, in fact, programs that are notably already compliant and have been taking compliant transactions for a while. For example, I believe Idaho has been taking compliant transactions since January. But there are others that are struggling right now.

The good news is that all plans, all State Medicaid agencies, have already instituted contingencies. So even though they are still working toward compliance, they have plans to continue payment.

The CHAIRMAN. Will Medicaid programs also be covered under CMS' contingency plan?

Ms. ADAIR. No. Each State would themselves deploy the contingency.

The CHAIRMAN. OK.

Ms. ADAIR. What I mentioned today was specific to Medicare. Each Medicaid State agency, is responsible for deciding what their contingency is, as well as for deploying the contingency.

The CHAIRMAN. Do you anticipate much of a revision by doctors to paper claims?

Ms. ADAIR. I want to separate the conversation here of Medicare to all others.

The CHAIRMAN. Yes.

Ms. ADAIR. I will deal with the Medicare one first, if I might.

The CHAIRMAN. Please.

Ms. ADAIR. As you would certainly know, the ASCA legislation had a provision in there specifically on Medicare that said that, effective October 16, all claims should be submitted to Medicare electronically. There were two exemptions, notably for physicians' offices that are less than ten FTEs, as well as facilities with less than 25 FTEs, and would be allowed to continue to submit paper claims. But everybody else was required to submit electronically.

So the answer to the question for Medicare is that we do not foresee much of a revision to paper.

The CHAIRMAN. How will the contingency plans impact this?

Ms. ADAIR. As you know, sir, Medicare has a very high percentage of claims coming in electronically, and since people would be allowed to continue in the legacy formats, it should have no impact there.

For the rest of the industry, going back to paper will be driven by two things. No. 1, going back to paper would be very difficult for some providers if they were already submitting electronically. Reverting to paper would have them change many of their business practices, which I don't think they would want to be doing. Second is that providers may have contract arrangements with the plans that may not allow them to go back to paper.

The CHAIRMAN. Let me switch now, because I think we're building an important record here that a few folks are going to be reading in the next few hours as we move toward these deadlines. This goes beyond that now to a statement you made about a $30 billion savings.

What are CMS' current projections, if any, of the overall cost of system-wide compliance with the HIPAA transaction requirements to hospitals and doctors, et cetera?

Ms. ADAIR. Well, the $30 billion was an estimate that was done back in the impact analysis with the August 2000 rule, which promulgated the standards themselves. What you're asking me, sir, is our experience in implementation——

The CHAIRMAN. That, because there's so many dollars out there for health care, and when we start diverting them to this kind of process and procedure, the natural reaction is they get diverted away from the patient and the care itself. I think that's going to be a growing concern here as we look at the overall cost of compliance.

Ms. ADAIR. In our impact analysis we acknowledged, and I think continue to acknowledge, sir, that in the first couple of years we would experience the cost of change, change to these electronic formats, to these standards, to these new code sets, and that we

would be experiencing a cost, and I think we have brought that to bear.

The anticipation—and I think we still believe it—is that once we have, in fact, overcome the cost of change, the benefits will, in fact, be there.

The CHAIRMAN. Well, that is the flip side and that's obviously fair to reflect on. That was going to be my next question.

Have you looked forward, beyond the bubble of cost, if you will, to the effect and the savings that the system might benefit from?

Ms. ADAIR. I think that every day, in conversations that we have with industry we assure ourselves that the benefits are, in fact, there. As I mentioned in my written testimony, when you take a look at what has happened in other industries, be it banking, be it the shipping industries, that the benefits of standardization, the benefits of inner-operability are there. It is the cost of change and the pain of change that is difficult to get through. So I believe we still do believe that the benefits are there.

When you take a look right now, where there are over 400 proprietary formats that insurance claims can be submitted in, getting down to the HIPAA standards, the benefits that that will bring to the back offices of a physician or a hospital are, in fact, very large and very significant for the health care industry. So as you point out, it does take money, precious money, to do it right now, but the long-term benefits and the ability not to be expending those things in the future, certainly I think the balance says that standardization is the way to go.

The CHAIRMAN. Well, we hope that is the case.

A couple of last questions to you, Miss Adair. CMS announced recently that it would pursue a relatively relaxed complaint-driven approach to enforcing the new transaction rules. Now, I say that because I think doctors and hospitals have labored for years under a very aggressive CMS and OIG enforcement of Medicare fraud and abuse rules.

What assurance should they have that CMS' approach to HIPAA will be different in the long run?

Ms. ADAIR. We have been hopefully very clear, sir, that the most important thing for us when we talk about enforcement of HIPAA is compliance, that that is the goal we are working toward. We have been clear that we're going to be working on a complaint basis. Our hope is that the industry begins to work out the issues of noncompliance, but that if somebody wants to come to us and file a complaint, we will, in fact, work with them to become compliant. We will talk to them about where the aberrancies are.

The legislation provided us the opportunity to work through corrective action issues before we ever got to a place where we would want to consider moving toward penalties, civil monetary penalties. So that our goal really is to exercise what was provided to us in the legislation, taking a look at corrective action measures before we move to any kind of negative activity.

The CHAIRMAN. I think a friendly CMS in that area of compliance will be well-received.

Even CMS itself concedes that only about 14 percent of its own Medicare transactions are currently HIPAA compliant. That is a disturbingly low number, considering we're just weeks away. Even

assuming that implementation of contingency plans provide for temporary acceptance of non-compliant claims, do you believe it is possible for the U.S. health system to be ready for full conversion to HIPAA compliance any time in the foreseeable future?

Ms. ADAIR. I think we are all responsible, sir, for continuing to do our best in outreach, getting people into testing, so that we dramatically improve what you point out is a very low number of claims in production. We are hopeful. It is true the number you cite, 14 percent of claims in production right now.

The number of providers is somewhat higher, and the number of providers in testing is also somewhat higher. We believe that on October 16 the number will shoot up a little bit, but obviously, our opinion was certainly not enough to not deploy the contingency. But we will continue to work with folks and we do believe that, in our history, with changes of formats, that we see a steep curve at the very last moment, but we did not believe that it was adequate to not deploy our contingency, not putting those payments at risk.

The CHAIRMAN. My last question of you—and obviously, we're seeing the scope of this regulatory process and moving toward compliance. How long do you think it will take for the full system to achieve HIPAA readiness, and what additional steps will CMS and the industry need to achieve to gain this goal?

Ms. ADAIR. I believe that we have formed very good working relationships, sir, with the industry. We have been working with the associations, both for payers, plans, as well as provider organizations, associations. We will continue to be working with them to stress the importance of compliance, and we will be working with them, sharing with them the statistics that we have on both Medicare, and hoping they share their statistics with us, of those people that are testing, the issues that they are having in testing, and those as they move toward compliance.

It is not until we see the results of those efforts that we could make a projection as to what is the date that we thought we believed we should drop our contingency.

The CHAIRMAN. Director Adair, let me thank you for your thoroughness today and your openness to obviously these very real concerns that are out there across the industry at this moment.

Ms. ADAIR. Thank you for the opportunity.

The CHAIRMAN. I think your announcement today and the announcement of Director Scully come as a degree of relief, but a clear recognition that, because of the character of the law and its intent for implementation, there's going to have to be a push forward. I think that cooperative working relationship, helping systems through this, is a good deal better and a way for our government to approach this problem than to immediately start actions and compliance enforcement that recognizes fines and penalties. That is not the way to go here as we nudge this process along and bring it into compliance.

We still have small practitioners out there that serve our communities and our citizens extremely well. Driving their costs up and the complexity of their operations up is not necessarily a way to achieve success and/or quality health care. So we thank you very much.

Ms. ADAIR. Thank you.

The CHAIRMAN. Rick, thank you for your patience. Let me follow up with a similar line of questioning to you, because your testimony touches on some areas where the new Privacy Rules have triggered confusion or disruption amongst patients and providers. Clearly, what you have outlined this morning and the response to your web page and the clarifications appear to be working, or at least certainly being reacted to. Whether they're working out there or not, or whether they're clarifying action within the waiting room, if you will, is yet to be seen.

Nevertheless, because I and my colleagues continue to receive numerous complaints, I would like you to clarify, as specifically as you can, what the new rule does or does not require in a few key areas.

These are, to what extent are providers free to share patient information with other providers?

Mr. CAMPANELLI. Well, that first one, Senator, is the one I alluded to in my opening remarks. We have a good treatment of it in the testimony and in the FAQs, which I recommend that everybody visit.

The answer is that providers are quite free to share patient information with other providers for treatment and that means doctors can share freely with other providers without having to get advance written consent from any person. I think that's the area where you may have heard reports of confusion on that.

The CHAIRMAN. Yes.

Mr. CAMPANELLI. I will say that the anecdotal reports we were getting of this early on, after April 14, we heard more of that initially than we're hearing now. I think there's a couple of reasons for that.

First of all, we went out of our way to make it clear in the modifications that providers can share this information freely with other providers for treatment purposes. There are specific elements of the rule that provide this ability to freely share x rays or other diagnostic information with other providers.

Second, we have guidance and FAQs specifically on this topic up there. The word we're getting is that when a provider is told by another provider that he can't have that information, he tells them "yes, I can", and this is why.

The CHAIRMAN. Then this question. Are doctors at risk if they use informal or unsecured methods of communicating with each other, such as phone calls, e-mails and faxes?

Mr. CAMPANELLI. Well, the Privacy Rule requires that reasonable safeguards be adopted in transmitting information. But in most of those cases that you just described—faxes to a number that is routinely being used, phone calls to talk to a doctor, to another provider—certainly in all those cases that, of itself, would be permitted under the rule. It requires reasonable safeguards which the fax case, would likely be that you confirmed the correct fax number. So on our guidance on the web, we particularly talk about the ability of doctors to fax information to others for treatment purposes. We make that quite clear.

The CHAIRMAN. Where, if at all, is it required under the rules for hospitals or other entities to deny information about patients to families or friends, to clergy, and what about law enforcement?

Mr. CAMPANELLI. Well, taking them in order, the rule certainly does not prohibit the sharing of that information. Now, the rule does, as you recognize, adopt provisions which protect the privacy of health information. That means that in many of those cases what we do is we start out with a requirement that the information be protected, unless there are provisions in the rule that allow it to be disclosed. But we have particular provisions in the rule that permit information to be shared with friends and family members, or even anyone who the individual patient identifies as being involved in their care.

So in those cases where the patient does not object, the rule makes it clear that a doctor can share that information with friends, family members, others identified as involved in the care relevant to the treatment or even to payment, to helping the person obtain payment.

Let me give a little bit more information about that, if I can, because there has been some confusion, where people have asked, "well, what if the patient is not conscious or not present?" In that case, the rule permits unless the patient has opted out, has expressed some indication before that they don't want the information to be shared—the treatment provider or the other covered entity to make that decision in the best interest of the patient. So whether the patient is there and conscious, or the patient is not there, the information can be shared when appropriate.

The CHAIRMAN. Are patients required to accept the new privacy disclosures that doctors are giving out at doctor's visits before care can be provided?

Mr. CAMPANELLI. I'm sorry. Say that again, Senator.

The CHAIRMAN. Are patients required to accept the new privacy disclosures that doctors are giving out at doctor's visits before care can be provided?

Mr. CAMPANELLI. I think what you're referring to is the Notice of Privacy Practices that the rule has. If you've been to the doctor, I know you have received one, and you've gotten one from your health plan as well.

The answer is that patients are not required to accept them as a condition of treatment. In fact, all that's required is for the doctor or the other provider to provide the notice and make a good faith attempt to obtain the patient's acknowledgement of having received the notice. If the patient doesn't want to sign that acknowledgement, the doctor or other provider can merely note that they've made an attempt to obtain the notice acknowledgement from the individual. It is certainly not a condition of treatment to the individual.

The CHAIRMAN. But that kind of information must be within the file to hold the doctor harmless?

Mr. CAMPANELLI. Well, the requirement is that the doctor or other provider make a good faith attempt to obtain a written acknowledgement or document why it was not obtained, so it would be prudent to just note that "I attempted to get the person's acknowledgement—" you know, someone in the office, not necessarily the doctor, but someone in the office to note that the attempt was made to get it from the individual.

We've seen this happen in a wide variety of ways. The rule is quite flexible and scalable, as we say, about how this can happen. Sometimes there's a form that a person signs when they get the notice initially. They can sign it, and that is either handed back in, or if the patient declines to do it, then the appropriate person there at the office can just note that the patient declined to acknowledge receipt of the notice.

You know, I realize I didn't answer one of your questions before that you asked. You asked me about clergy.

The CHAIRMAN. Yes.

Mr. CAMPANELLI. Would you care for me to go back to that?

The CHAIRMAN. Please, and law enforcement.

Mr. CAMPANELLI. Law enforcement.

First, clergy. I was talking earlier about the opportunity in the rule, permission in the rule, for providers to share information with friends, families, or individuals. Well, clergy, similarly, of course, can receive information. But there has been some confusion in the clergy arena with the issue of hospital or facility directories, as they're referred to in the rule.

Can a hospital have a directory of patient information?

The answer is the rule envisions and anticipates that hospitals or other providers will have this directory of patient information, where the patient has the opportunity to be included or to opt out of having their information included in a directory, and the patient can also include, for instance, religious affiliation. So any member of the public—not just clergy, but any member of the public—can come in, ask about the patient, and if the patient has opted to be included in the directory, just like now, just like we're all used to, receive information about the patients location in the hospital, and general condition.

In addition, clergy can view the directory without having to have the name of the person. They don't have to ask for the person by name, and they also can get the religious affiliation information. So we are very solicitous of and very careful to emphasize that individuals, friends, family, loved ones, others involved in care or clergy, can get the information.

Let me mention that very early on, shortly after the compliance date, we got a call from a reporter actually that said a woman in one State had gone to a hospital to see her husband and was told that she was not allowed to see her husband because of HIPAA. I said, well, I don't think there's anything in HIPAA that prevents this. So I asked the reporter to go back and get a little information.

Well, it wasn't HIPAA, it wasn't the hospital, so we wondered if the husband had actually declined to see the wife. It is not HIPAA. HIPAA permits opportunities to share information with spouses with families, and with clergy.

Now, law enforcement. Let me go to that.

The CHAIRMAN. Yes.

Mr. CAMPANELLI. There are a variety of circumstances under which law enforcement can have access to information. Again, this is an example where the Privacy Rule balances two key interests. A very important interest, which I know you recognize, is the privacy of personal health information, and also in this case the interest of law enforcement to carry out their important responsibilities.

There are a variety of ways that law enforcement can have access to the information. For instance, information that is required by law to be disclosed may be disclosed to law enforcement. Reporting of gunshot wounds which, State law typically requires is permitted. Also, of course, where there's a court order or a warrant, the Privacy Rule permits that disclosure to occur.

In addition, there are a variety of circumstances outlined in the rule that allow law enforcement to have access to this information. For instance, for the purpose of identifying or locating a suspect, a fugitive, a material witness or a missing person, that information is permitted to be shared with law enforcement.

PHI, Protected Health Information about victims of a crime in response to law enforcement's request can be shared with law enforcement if the individual agrees. Protected Health Information about a decedent can be shared with law enforcement if there's a suspicion that death resulted from criminal conduct. Evidence of a crime that occurred on the covered entity's premises can be shared with law enforcement. So if there's an investigation going on right there about a crime, that can occur.

If there is a provider on the scene of a medical emergency—for instance, let's say there's a covered entity that's an ambulance driver or company that is on the scene responding to a medical emergency, they can share information with law enforcement about the criminal activity, such as the nature and location of the crime, the location of victims, identity description, location of the perpetrator of the crime. So we have really tried to make it clear.

We have heard of some areas where there's a misconception about this. But there's an array of particular balances in the rule where law enforcement is permitted to get this information, to permit law enforcement to continue. Our effort is to try to get the word out about this to law enforcement.

A lot of law enforcement jurisdictions understand this. We have seen some areas where there's confusion on this and we've tried to be in touch with them.

The CHAIRMAN. Are doctors subject to lawsuits if they inadvertently disclose protected information?

Mr. CAMPANELLI. There is no private right of action in HIPAA against doctors for violation of the rule.

The CHAIRMAN. In your testimony you cite CMS estimates projecting the cost of compliance by the Privacy Rule in the neighborhood of $12-$17 billion over 10 years, and I'm sure you are aware that some private estimates put the cost quite a bit higher than that.

Recognizing that, even before the new Privacy Rule, providers were already bound by the requirements of patient confidentiality, how much of a significant improvement are the new rules, and are they worth the upwards of $17 billion of the already scarce dollars we have discussed throughout this hearing?

Mr. CAMPANELLI. Let me say, Senator, that we are certainly sensitive to the cost issues about this. I think there was an understanding when Congress mandated or created the process by which the Privacy Rule would be created that there would be significant costs associated with it, and that they would be outweighed, it was

thought, and we still believe, in the context of the cost savings from administrative simplification.

One thing I would say. It's true that there are protections of privacy, laws to protect the privacy of medical information, that exist in various jurisdictions throughout the country. But they are really a patchwork of laws, and in many jurisdictions there is no protection at all. So certainly one of the key benefits of the Privacy Rule is to establish a Federal foundation of protection for those rights, and to make clear what those rights are.

Like I mentioned before, the rights of access, the right to request an accounting of how disclosures are made and the right even to make a correction to the record, to name just a few; the right to make sure the information isn't disclosed for marketing purposes, or to employers, in violation of the rule. All of those are very important rights.

I think our citizens are well-served by knowing that they have those rights, and many, I think when they're reading the notices of privacy practices that they receive, really have realized for the first time what is at stake here and what rights they have available. So we are convinced that the rights that are afforded now under the Privacy Rule are significant and essential to the protection of privacy of our citizens.

We recognize there are costs, as Jared said, with respect to the CMS circumstance. There are significant startup costs associated with this and we recognize this. But we think, over time, and we expect—and we are working toward this end—that the protections of the rule and the requirements of the rule will really become understood as part of the fabric of how health care and payment are done and people will understand them better.

The CHAIRMAN. Your testimony stresses that HHS is trying a primarily compliant-driven approach to enforcement, with an emphasis on informal resolution. Yet, recent reports indicate that HHS has begun forwarding HIPAA privacy complaints to the Department of Justice for criminal prosecution.

How much of this is going on, and how does this fit with the policy of informal resolution?

Mr. CAMPANELLI. Well, I think it's completely consistent with it, Senator. You know, as I'm sure you recognize, some of the provisions of the rule, a subset of provisions of the rule, are subject to criminal penalties. HHS has responsibility for enforcement of violations of the rule that are subject to civil penalties, and the Department of Justice is responsible for violation of the rules that are subject to criminal penalties. So our referral of these cases to Justice reflects the fact that these are really within the purview of the Department of Justice to pursue them.

The CHAIRMAN. The process for referral is that you have already made a determination that you believe these could be criminal in nature, not civil?

Mr. CAMPANELLI. That's correct, to this extent. There are elements of the rule—for instance, disclosures that are a knowing disclosure of protected health information in violation of the rule, those are potentially subject to criminal penalties. It is the Department of Justice that imposes those. So in terms of our review, we

intake cases and sometimes it takes a little bit more information for us to determine what is really the nature of this complaint.

But where a matter has arisen and it is apparent that it is subject to criminal violations, then those are appropriately dealt with by the Department of Justice and we refer them to the Department of Justice.

The CHAIRMAN. Despite its huge size and complexity, the Privacy Rule nevertheless relies heavily on some very general standards, such as what a doctor may reasonably infer or requirements to provide only minimum amounts of information necessary.

What steps can HHS take to give providers and patients the guidance they need to understand what these broad terms actually mean in real world resolution?

Mr. CAMPANELLI. Yes, Senator. We are sensitive to that. You know, I just want to step back a bit for a minute and say why is it like that.

I think one of the reasons is that the rule, as I said before, attempted to be flexible and scalable. We recognize that the covered entities who are subject to the rule run everywhere from the small provider that you talked about in a rural office, in a remote location, to major institutions. What is appropriate and reasonable in the context of one would not be appropriate and reasonable in the context of others. So that's why the rule necessarily, and I think appropriately, includes references to reasonable safeguards, because we recognize that many of these things are not only relevant to the size of the provider but to the particular context. Really, you have to look at the circumstances to see what's appropriate.

Now, how can we help with that? Well, I think that's where our guidance has really come in and been welcome. In fact, the rule in some cases makes it clear. For instance, I mentioned with respect to providers' sharing x rays and other diagnostic information for treatment. It is in the Privacy Rule where it says that this information can be shared with reasonable safeguards.

But in our guidance we try to give examples, helpful examples, as much as possible, where we have been able to identify, for instance, in a semi-private room, that a doctor who is talking in a semi-private room should adopt reasonable safeguards. That may mean lowering his voice in the room. You know, we have offered that kind of information.

Or about medical charts. We have seen some confusion about medical charts. People have said you can no longer have medical charts on the wall on a patient floor. Well, it depends on what other safeguards you can bring to bear on the case. Many times a completely reasonable circumstance will be just to make sure that any identifying information is facing the wall.

So in answer to your question, with the particular FAQ guidance or our extensive guidance that's on the web right now, where we have narratives and examples, that's what we're trying to do. When we hear from folks that they need more assistance, we have tried to be responsive to that.

I might just add that we are also in the process of developing targeted information or guidance to particular segments of the industry. For instance, small providers are likely to be one of those groups.

The CHAIRMAN. You mentioned earlier, in response to a question, the hodgepodge, if you will, of States and the creation of uniformity that this provides. In some instances State laws are more stringent than HIPAA.

Mr. CAMPANELLI. Yes.

The CHAIRMAN. They argue that it's very difficult to assess in practice.

Do you see this as a serious problem? What steps is HHS taking to provide guidance regarding State preemption?

Mr. CAMPANELLI. First, I confirm that the Privacy Rule defers to more stringent State standards for the protection of privacy. So that's correct. That means if a particular State has a more stringent standard——

The CHAIRMAN. Equal to or greater than.

Mr. CAMPANELLI. That's right, sir. In that State then, if there is a higher standard for the protection of privacy with respect to a disclosure or the use of personal health information, that higher standard would apply. Obviously, that will vary from jurisdiction to jurisdiction.

The Privacy Rule defers to States where they have opted to take a higher or a more stringent position as to the protection of health information.

Also, though, I want to say that in some circumstances we are able to help covered entities comply where they have to look to both State and local law. In fact, just recently, I think just at the beginning of this month, in September, we put up on the website a frequently asked question that helped organizations and covered entities understand how they can more easily and readily incorporate the State law into their Notice of Privacy Practices, so that if they are a multijurisdiction covered entity, they don't have to completely redo the entire Notice of Privacy Practices every time a State law changes. We tried to come up with a reasonable way where covered entities could reflect the more stringent State standards and just change that appropriately in a more narrow way, rather than having to change everything. We are sensitive to that issue.

The CHAIRMAN. To both of you, thank you very much, Dr. Campanelli, Director Adair. Thank you for your presence here today and your forthrightness and testimony. I think we have built a valuable record here and some extremely valuable information has flowed this morning.

As you know, that is part of the responsibility of this committee. We are a nonauthorizing committee, but we do work to build a record for the other committees to use, and finance is certainly one of those who uses us very readily, as informational sources in looking at compliance or in looking any adjustments or changes within current law. Again, we thank you very much for your time here this morning, and we will excuse you.

Ms. ADAIR. Thank you.

Mr. CAMPANELLI. Thank you, Senator.

The CHAIRMAN. I will now ask the second panel to come forward, please. Next let me welcome our second panel.

Cathy Treadway is a Medical Practice Administrator from Boise, ID. She has been very active in helping coordinate HIPAA prepara-

tion efforts statewide and is, I am told, one of Idaho's best experts on this extremely difficult subject.

Mary Grealy is President of the Healthcare Leadership Council, which is, as its name suggests, a leading voice for America's health care industry, including providers, payers, and health care entities and companies.

Alissa Fox is Executive Director for Policy for the Blue Cross/Blue Shield Association of America, and will talk with us about how the health plan community is responding to HIPAA, in particular the new transaction standards.

Finally, Janlori Goldman is Director of the Health Privacy Project, perhaps the country's most prominent non-profit advocacy organization, focusing on patient privacy issues.

We welcome you all. Cathy, you came the furthest, I think, so we will allow you to go first. We do appreciate you coming out from Idaho to be a part of this record. Please proceed.

STATEMENT OF CATHY TREADWAY, MEDICAL PRACTICE ADMINISTRATOR, THE WOMAN'S CLINIC, BOISE, ID; APPEARING ON BEHALF OF THE MEDICAL GROUP MANAGEMENT ASSOCIATION

Ms. TREADWAY. Good morning. I am Cathy Treadway, the Administrator of the Woman's Clinic, a nine-physician, 65 employee specialty OB/GYN practice in Boise, ID. I am a member of the Medical Group Management Association and have held several leadership positions in the Idaho MGMA. MGMA is the Nation's oldest and largest medical group practice organization, representing more than 19,000 members who manage and lead 11,000 organizations, in which approximately 220,000 physicians practice.

I would like to thank Chairman Craig and the committee for convening today's hearing on HIPAA implementation. Over the past 2½ years, I have dedicated considerable energy to increasing my knowledge of the HIPAA regulations and helping to educate providers throughout Idaho as a member of the Idaho HIPAA Coordinating Council. While I will be commenting briefly on the HIPAA Privacy Rule, I will focus particular attention on the electronic transactions and code sets, the TCS Rule.

I would like to begin by discussing the implementation costs which practices already have incurred and will continue to incur in the future.

Examining just our small practice, the Privacy Rule implementation costs total in excess of $10,000. Like practices throughout the country, we struggle with limited resources to deal with the magnitude, complexity and costs of HIPAA implementation. I must emphasize that these are just the initial Privacy Rule implementation costs. There are significant ongoing privacy costs for each practice, including continuing education, training of staff and physicians, printing and facility modifications.

Practice costs for TCS implementation typically include new HIPAA compliance software, computer hardware, staff training, education materials, and for my practice, additional claim costs averaging $500-$600 per month. In addition, there are numerous future HIPAA standards scheduled for implementation. These include national identifiers, electronic claim attachments, and secu-

rity. Each of these standards will demand additional implementation costs. These expenses must be considered in conjunction with the many unfunded mandates group practices face: projections of decreasing physician reimbursement and sky-rocketing medical liability premiums.

It is imperative that both Congress and the Administration not examine the effect of any one regulation in a vacuum, but consider the cumulative effect that government decisions have on patient access to quality care.

Let me briefly discuss the privacy regulations. While some uncertainty regarding particular aspects of the rule remains, it is important to note that we have not encountered any significant problems from patients. Rather, the continuing challenges stem from provider misunderstanding, misinterpretation, and uncertainty in complying with the rule's requirements. I have outlined these lingering issues in my written statement.

I now wish to discuss the migration to the HIPAA standards for TCS. Along with providers around the Nation, I am fearful that cash-flow will be disrupted following the mandated compliance date of October 16.

I have highlighted in my written statement my concern regarding the current readiness level of most group practices throughout the country. I would like to note, however, that many of the members of this committee represent States with large rural populations and, as such, I believe providers in those jurisdictions share many if not all of my concerns.

According to an informal survey that I conducted, many Idaho health plans are just beginning to test claims with their provider customers. As a result, the vast majority of Idaho health practices do not feel that they will be ready to submit HIPAA compliant claims by October 16. In addition, some software vendors are requiring providers to process their claims through a proprietary commercial clearinghouse, thus incurring a per-transaction charge. The result is yet another unanticipated and ongoing cost for providers.

In my own practice, we have experienced significant claims testing challenges. During our initial round of testing, the rejected claims contained no specific error information. Thus, we had no idea if the error was with our own software, our clearinghouse, or potentially non-compliance on the part of our health plans. As of September 19, last Friday, our vendor-designated clearinghouse has yet to schedule testing with some of the largest health plans in the State, including Blue Cross of Idaho, Regence Blue Shield, and Idaho Medicaid. How can we even hope to be paid by our payers after October 16 when we cannot even test our claims? Fears of payment delays are exacerbated by the fact that in States without prompt payment laws, such as Idaho, there is no incentive for health plans to pay claims expeditiously. In addition, Idaho Medicaid cannot accept both legacy claims and HIPAA compliant claims. It is HIPAA compliant or their software or paper claims.

Our continuing concern with the lack of industry readiness led MGMA and almost 40 other provider organizations to request the government issue a definitive statement to the industry regarding enforcement of the TCS standard. On July 24, HHS responded with

guidance regarding the enforcements of the HIPAA TCS standards after October 16. The HIPAA statute requires covered entities to comply with TCS by October 16. By restating that fact while also outlining some conditions under which CMS will not impose penalties, the agency sent health plans conflicting messages in the July 24 guidance. Consequently, some health plans believe that they are legally compelled to reject noncompliant transactions. This quandary is particularly problematic for those health plans that will not be compliant until shortly before the deadline and, therefore, are not in a position to engage in provider testing until that point. However, the guidance did send a signal to health plans that they should make every effort to continue the cash-flow for their provider customers.

CMS bolstered this enforcement flexibility position with the publication of a set of Frequently Asked Questions on September 8. In them, CMS states that a contingency plan for a payer could include not only the acceptance of legacy claims, but also flexibility in terms of data content and the offering of interim payments.

Legacy claims are those that CMS and private plans currently accept. Exercising data claim flexibility would allow the government and private sector plans to process and pay claims that do not include all the required data elements. While MGMA was pleased to see this turn around, we believe CMS must explicitly tell noncompliant health plans that failure to develop appropriate contingencies to prevent cash-flow disruptions is unacceptable and is grounds for immediate enforcement action.

Regarding TCS, CMS should first instruct its intermediaries to continue processing noncompliant claims after the October 16 deadline. We are pleased to hear this morning the announcement regarding CMS contingency plans. However, CMS needs to clarify that all public and private health plans are permitted to accept, process and pay HIPAA compliant claims with fewer data elements than required.

Second, CMS should strongly encourage health plans to return claims to providers with an explanation of any data content deficiencies in a timely manner. This will permit the entry of missing data and prompt resubmission of claims.

Mr. Chairman, while MGMA is confident that complete HIPAA implementation will eventually ease some administrative burdens and facilitate improved data inter-change within the health care community, significant roadblocks continue to exist. MGMA, along with Idaho MGMA and IHCC, believe our recommendations will help providers manage this difficult transition.

We urge Congress to play an active role in ensuring that the administration takes the necessary steps to avoid interruptions in the delivery of care.

I appreciate the committee's interest in this important topic and thank the committee for inviting me to present my views on this issue.

[The prepared statement of Ms. Treadway follows:]

MGMA Center for Research
American College of Medical Practice Executives
Medical Group Management Association

STATEMENT

of the

Medical Group Management Association

to the

Special Committee on Aging

U.S. Senate

HIPAA Medical Privacy and Transaction Rules: Overkill or Overdue?

Cathy Treadway, FACMPE
The Woman's Clinic
Boise, Idaho

September 23, 2003

Good morning. I am Cathy Treadway, FACMPE, the administrator of The Woman's Clinic, a nine-physician, 65 employee single-specialty obstetrics/gynecology practice in Boise, Idaho. Our clinic is the oldest specialty clinic in Idaho and was established in 1946 by Harold Dedman and Verne Reynolds, pioneers in the formation of the American College of Obstetricians and Gynecologists (ACOG). We currently deliver approximately 1,700 babies a year and provide care for thousands of women throughout their lifetime.

I am a member of the Medical Group Management Association (MGMA) and a fellow of the American College of Medical Practice Executives. MGMA is the nation's oldest and largest medical group practice organization representing more than 19,000 members who manage and lead 11,000 organizations in which approximately 220,000 physicians practice. MGMA's membership reflects the full diversity of physician organizational structures today.

MGMA's individual members, who include practice managers, clinic administrators, and physician executives, work on a daily basis to ensure that the financial and administrative mechanisms within group practices run efficiently allowing physician time and resources to be focused on patient care. MGMA members are uniquely qualified to assess the direct impact of the Health Insurance Portability and Accountability Act (HIPAA) on providers and the delivery of quality care to beneficiaries.

I have held many positions in the Idaho MGMA, including President and Scholarship Chair. In my current position, I represent medical practice administrators and physicians on the Idaho HIPAA Coordinating Council (IHCC). The IHCC, a state affiliate of the Workgroup for Electronic Data Interchange (named in HIPAA as an advisor to HHS), represents those who are impacted by HIPAA. IHCC members include representatives of health care providers, insurance carriers, third-party billing agents, and state, county and city governmental entities. The IHCC provides the means to create a collaborative healthcare industry-wide process to bring about a statewide coordination effort that is necessary to achieve successful HIPAA compliance. IHCC has conducted a series of seminars to educate Idaho providers, hospitals, and other entities covered by the HIPAA regulations.

On behalf of MGMA, I would like to thank Chairman Craig and the committee for convening today's hearing on HIPAA implementation. While I will be commenting on aspects of the HIPAA privacy rule, due to the looming October 16 deadline, I will focus particular attention on electronic transactions and code sets (TCS).

As a group practice administrator, my tasks include: financial management, recruitment and orientation of physicians, patient advocacy, employee supervision, regulatory compliance, marketing, facilities management, and contract negotiation. The physicians in our practice rely on my expertise to guide them through innumerable and continually changing federal rules and regulations, including HIPAA, coding, documentation, billing, physician referral rules, local Medicare review policies, physician credentialing, and assignment and reassignment of patient and physician billing rights. As most physician time is consumed by providing and documenting patient care, they depend upon my business acumen to maintain the smooth daily operations of the practice.

Over the past 2 ½ years, I have dedicated considerable energy to increasing my knowledge of the HIPAA regulations, striving to bring our practice into compliance, and helping educate providers throughout Idaho. Like practices throughout the country, we struggle with limited resources to deal with the magnitude, complexity and costs of HIPAA implementation.

HIPAA Standard for Protecting the Privacy of Health Information

For many years, physicians have placed the highest priority on protecting the privacy of patients' health information. The HIPAA privacy rule serves as an important tool to ensure that each patient's privacy is sufficiently protected by every sector of the health care community. The requirement to educate each staff member on a patient's right to privacy has increased the overall level of awareness in our industry regarding the importance of maintaining privacy.

While I found, and continue to find, aspects of the HIPAA privacy compliance process challenging, my task would have been even more difficult without the positive changes made to the original consent requirement by the current Administration. The rule's current approach allows us to continue to provide care to our patients with minimal delays. Adding a consent form to the already unmanageable paperwork burden practices face would not enhance patient privacy. Conversely, the original consent provision would have interfered with the routine administration of health care, delayed patient care, and created confusion among patients and physicians alike.

Ongoing Challenges and Costs

Preparing for the April 14, 2003 compliance date was a most trying time for most practices, as it took several hundred hours of dedicated effort. Some uncertainty regarding particular aspects of the rule remains. It is important to note that we have not encountered any significant problems from patients. Rather, the continuing challenges stem from provider misunderstanding, misinterpretation and uncertainty in complying with the rule's requirements.

Patient Consent

The privacy rule permits practices to disclose health information without a patient's consent for purposes of treatment, payment, and health care operations. Unfortunately, some practices are refusing to release information for these purposes without a patient's consent. For example, a common scenario involves patient referrals to physician specialists, where the disclosure pertains to treatment and thus the patient's consent clearly is not required. Much of this confusion seems to originate from the rule's initial consent requirement. Practices fear that they will improperly release information without a patient's consent and be assessed penalties as a result. This confusion creates unwarranted delays in providing needed care to patients.

Notice of Privacy Practices

Physician groups must provide a "notice of privacy practices" to every patient and make a good faith effort to obtain a written acknowledgment that the patient received the notice. The notice describes a group's privacy policies and procedures, a patient's rights, and to whom health information may be disclosed. There appears to be some uncertainty regarding how to satisfy the aforementioned requirements. Some groups are providing patients a hard copy of the notice, while other groups are choosing to laminate copies of the notice for patients to read in the waiting room.

Preemption

In addition to the time and effort required to understand the HIPAA privacy rule, practices must also examine state medical privacy laws (including regulations, case law, etc.). Because the privacy rule only preempts less stringent state laws, practices must compare both the HIPAA privacy rule and state law as part of their compliance efforts. As you can imagine, this is a daunting task for our small Idaho practices. In addition, due to the complexity of a preemption analysis, there is a concern that practices will reach different conclusions regarding which requirements to follow - federal or state.

Costs

Examining just our small practice, the privacy implementation costs total in excess of $10,000. I must emphasize that these are just the initial privacy implementation costs. There are significant ongoing costs for each practice, including continuing education, training of staff and physicians, printing, and facility modifications. These expenses must be considered in conjunction with the many unfunded mandates group practices face, projections of decreasing physician reimbursement, and skyrocketing medical liability premiums. It is imperative that the Congress and Administration not examine the effect of any one regulation in a vacuum, but consider the cumulative effect that government decisions have on patient access to quality care.

MGMA Privacy Recommendations

Develop Additional Guidance - The Office for Civil Rights (OCR) has made great strides in its outreach efforts to assist practices and all covered entities in complying with the privacy rule. MGMA urges OCR to continue to develop additional guidance to clarify the ongoing issues which affected parties identify.

Develop a Preemption Analysis - MGMA urges OCR to develop and maintain a preemption analysis that can be utilized by physician practices. OCR guidance in this area would ensure a uniform application of the HIPAA privacy rule and state privacy laws. The Congress should allocate necessary funds to enable the agency to conduct a preemption analysis and continue other important compliance outreach activities.

HIPAA Standards for Electronic Transactions and Code Sets

While the HIPAA standards for electronic transactions and code sets (TCS) are a long overdue re-engineering of the business side of the health care system, the migration to this new system has proven to be particularly demanding for physician practices. Successful deployment of HIPAA's electronic data interchange (EDI) standards has depended heavily on coordination between critical trading partners - providers, vendors, clearinghouses, and health plans. However, developing these partnerships and coordinating implementation strategies has been somewhat elusive in an industry often known for acrimony.

While MGMA is fully committed to advancing the widespread adoption of electronic data interchange, we are also concerned about the financial relationship between providers and health plans. For practices, failure to implement these standards could mean more than experiencing government enforcement action - timely reimbursement from health plans, the financial lifeblood of every provider organization, could be severely impacted.

Industry Readiness

With less than one month until the October 16 compliance date, MGMA has great concern regarding the readiness level of each sector of the health care industry. Surveys indicate that significant numbers of covered entities and vendors are either non-compliant or have yet to begin the testing of claims. In addition, there is great concern regarding the readiness level of both government-sponsored and private health plans.

Medical practices had anticipated and in many cases been assured that their practice management system software vendors would provide "HIPAA-compliant" solutions. In some cases, practice management system vendors will not offer their medical practice customers HIPAA-compliant connectivity between the practice and health plans by the October deadline. These delays have occurred for a variety of reasons. Certain vendors have made the appropriate software modifications, but have not found time to test them. Other vendors may not be able to complete all the required software revisions until well after the deadline. In other cases, vendors have not offered any HIPAA solutions to their customers.

Exacerbating the problem, certain vendors have already decided not to offer their medical practice customers direct connectivity with payers. Instead, they have required their customers to use a proprietary clearinghouse to submit electronic claims resulting in additional expenses to a practice. Concern also exists with the readiness level of health plans. With many health plans focused specifically on the October compliance date for their own systems, few have aggressively tested with their practice clients.

One of the reasons for the inability of health plans to initiate testing of provider claims in a timely manner was the delay in the Centers for Medicare & Medicaid Services (CMS) publication of the Addenda to the Implementation Guide - the first round of modifications to the TCS standard. This Addenda was not published until February 20, 2003, well after the original TCS compliance date of October 16, 2002. Most health

plan, clearinghouse, and provider software vendors waited for these changes before finalizing their products. This resulted in many health plans using virtually all the time available before the deadline to prepare their own organization for compliance. Although practices typically require at least three months to conduct such testing, in many cases they are only now beginning to start this process. Indications are that many practices will not have the opportunity to complete testing until well after the mandated compliance deadline.

In addition, there is great concern that many state Medicaid agencies will not meet the compliance deadline. Community health centers are typical of the organizations that rely heavily on Medicaid funds to sustain their operation. These entities are also the most financially vulnerable and can least afford to experience an interruption in their cash flow.

The Idaho Experience

According to an informal survey that I conducted throughout Idaho, a vast majority of practices do not feel that they will be ready to submit HIPAA compliant claims by October 16. Although they have been working to implement these standards, they have met many roadblocks. Many health plans are just beginning to test claims with their provider customers.

Most Idaho physicians currently submit claims electronically through Blue Cross of Idaho Clearinghouse or Regence Blue Shields Clearinghouse at no charge per claim. However, some software vendors are requiring providers to process their claims through a proprietary commercial clearinghouse, thus incurring a per transaction charge. The result is yet another unanticipated cost for providers.

In my own practice, we have experienced significant claims testing challenges. During our first sixty days of testing, rejected claims returned to us contained no specific error information. Thus, we had no idea if the error was with our own software, our clearinghouse, or potentially non-compliance on the part of our health plan. As of September 19, our vendor-designated clearinghouse has yet to schedule testing with some of the largest health plans in the state including Blue Cross of Idaho, Regence Blue Shield, and Idaho Medicaid. How can we even hope to be paid by our payers after October 16 when we cannot even test our claims? Fears of payment delays are exacerbated by the fact that in states without prompt payment laws, such as Idaho, there is no incentive for health plans to pay claims expeditiously.

Claim Format Errors versus Data Content Errors

Providers are aware that they must submit electronic forms using the HIPAA mandated ASC X12N format. However, the X12N Implementation Guide includes both "required" and "situational" information. Who decides when the "situation" calls for additional data? The health plans themselves. Providers and their software vendors have relied on health plans to announce how they have interpreted the Implementation Guides in what are termed "Companion Guides". Some health plans, however, have either not yet finalized their Companion Guides or have just recently released them. This led to delays

in software development, provider outreach, claims testing, and potentially the disruption of payment.

We continue to hear reports of health plans that believe they should require a much higher standard of perfection in claims submissions under the transactions rule than had previously existed. We are concerned that isolated mistakes will be considered violations of TCS standards and lead to the rejection of claims that would have been successfully adjudicated prior to October 16.

Insufficient CMS Guidance

On June 30, 2003, MGMA and almost 40 other provider organizations called upon the government to issue a definitive statement to the industry regarding enforcement of the transactions and code sets standard. On July 24, 2003, HHS responded with guidance ("Guidance on Compliance with HIPAA Transactions and Code Sets") regarding the enforcement of the HIPAA transactions and code set standards after October 16. The guidance clarified that plans which make a good faith effort to comply with HIPAA transaction and code set standards may continue to process legacy claims and permit claim data flexibility.

The HIPAA statute requires covered entities to comply with the standards for electronic healthcare transactions and code sets by October 16, 2003. By restating that fact, while also outlining some conditions under which CMS will not impose penalties, the agency sent health plans conflicting messages in the July 24 guidance. Consequently, some health plans believe that they are legally compelled to reject non-complaint transactions. This quandary is particularly problematic for those health plans that will not become compliant until shortly before the deadline; and therefore, are not in a position to engage in testing outreach efforts to providers until that point. However, the guidance did send a signal to health plans that they should make every effort to continue the cash flow for their provider customers.

CMS bolstered this enforcement flexibility position with the publication of a set of FAQs on September 8. In them, CMS states that a contingency plan for a payer could include not only the acceptance of legacy claims, but also flexibility in terms of data content and the offering of interim payments to their provider clients. While MGMA was pleased to see these pronouncements, we believe CMS must explicitly tell health plans that failure to develop appropriate contingency plans to prevent cash flow disruptions is unacceptable and is grounds for enforcement action.

MGMA Transaction and Code Sets Recommendations

Payment of Medicare Legacy Claims - We encourage CMS to instruct its intermediaries to continue processing non-compliant "legacy" claims after the October 16 deadline. Such instructions should indicate a specified period sufficient to allow all medical practices to complete testing. In addition, CMS should reiterate that all Medicaid and commercial health plans can continue accepting legacy claims.

Claim Data Flexibility - CMS should clarify that all public and private health plans are permitted to accept, process, and pay HIPAA-compliant claims with fewer data elements than specified in the maximum data set after the October 16 deadline. This clarification would dispel the notion that to comply with the law, health plans must reject claims with minor errors that would normally not impact the processing of the claim. In addition, CMS should clarify that claims with errors are still HIPAA standard transactions and cannot be rejected outright. Such clarification should indicate that minor errors that are not material to the processing of claims should not result in rejection of the claim, nor should entire batches be rejected because some individual claims in the batch contain errors or are not fully compliant with TCS standards.

Contingency Plan Publication - Medicare, Medicaid and all commercial health plans should announce publicly their contingency plans to allow providers sufficient time to implement business plans that ensure continued cash flow.

Delay Provider Enforcement - CMS should delay any enforcement action against providers until the provider community assures the agency that appropriate testing with health plans is completed.

Health Plans Must Report Missing Data to Providers - Health plans should return claims to providers with an explanation of any data content deficiencies in a timely manner. This will permit the entry of missing data and prompt resubmission of claims.

Medicaid Interim Payments to Providers - State Medicaid plans that will not be compliant by October 16 should offer providers an interim payment to avoid cash flow disruptions. This payment should be based on a calculation of the previous year's payments.

Health Plans to Prepare for Additional Paper Claims - CMS should encourage health plans to develop contingency plans to adjudicate a greater number of anticipated paper claims.

Conclusion

The burden of complying with both HIPAA privacy and TCS implementation has certainly strained our practice's staff and budget. Practices do not have the resources to survive significant payment delays, while continuing to provide care for all patients. Some practices have been pro-active - establishing lines of credit, delaying capital expenditures, setting aside cash reserves - hoping to weather delays in claims payment, meet payroll, and continue treating patients. It is clear, however, that resources may not be available to handle payment delays that extend more than several weeks.

While MGMA is confident that complete HIPAA implementation will eventually ease some administrative burdens and facilitate improved data interchange within the health care community, significant roadblocks continue to exist. MGMA, along with IMGMA and IHCC, believe our recommendations will help providers manage this difficult transition. We urge Congress to play an active role in ensuring that the Administration takes the necessary steps to avoid potential interruptions in the delivery of care. I

appreciate the Committee's interest in this important topic and thank the Committee for inviting me to present my views on this issue.

The CHAIRMAN. Cathy, thank you very much.

Now let me turn to Mary Grealy.

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

Ms. GREALY. Thank you, Mr. Chairman. Thank you very much for this opportunity to testify on the medical privacy rules that are part of the Health Insurance Portability and Accountability Act, HIPAA.

This is a matter of considerable importance to America's patients, health care consumers and health care providers, and I commend you for the attention that you are bringing to this important issue.

I am here today on behalf of the members of the Healthcare Leadership Council, a coalition of the Nation's leading health care companies and institutions. Our membership embodies all sectors of health care, and every one of our members is directly affected by the HIPAA Privacy Rules.

HLC also leads a coalition of over 100 organizations that strongly supports effective patient privacy protections.

Mr. Chairman, you called this hearing in part because of information you are receiving from health care providers about the cost and confusion associated with the HIPAA privacy regulations.

Let me say at the outset that we believe many of these difficulties could be avoided if Congress enacted a single national uniform standard for medical record confidentiality. What we have instead is a new Federal privacy regulation that does not replace the existing patchwork quilt of various State privacy laws but, rather, coexists with those laws. So no matter how well regulators write these rules, additional cost and lack of clarity is inevitable because doctors, hospitals and others are trying to navigate through a maze of Federal and State laws and regulations.

Having said that, let me specifically address the impact of the HIPAA Privacy Rules. To say these regulations are complex is an understatement, but that is, in part, because they are attempting to fulfill a difficult objective. How do we protect the sanctity of a patient's medical information privacy while at the same time ensuring that necessary information is available for providing quality health care and conducting vital medical research? The HIPAA regulations as revised by the current administration, while not perfect, do attempt to strike this necessary balance.

In terms of the value of these regulations, one point needs to be made. They do exactly what they are intended to do. Disclosing identifiable health information for purposes other than carefully defined, appropriate health care activities is strictly prohibited, unless the patient grants specific prior written authorization. If you disclose an individual's medical information to their bank, their neighbors, their employer, or their local newspaper, without their permission, you are going to be hit with Federal civil and criminal penalties.

These regulations, as I said, are not perfect, but they are an improvement over what they might have been. Under the original proposed regulations developed by the previous administration, patients would have had to give their written consent before they

could receive treatment, receive a reminder to make an appointment, have a doctor schedule their surgery, or even have a relative pick up a prescription. These rules would have generated treatment delays and volumes of unnecessary paperwork.

There are more improvements, though, that need to be made. As we revisit these rules—and there is a provision to have them reviewed and modified annually—we need to ask a critical question: do these regulations sap resources for unnecessary compliance activities, resources that could otherwise be devoted to patient care? The answer to that question is clearly yes.

HHS has estimated that the Privacy Rule will cost the private sector $17.5 billion over 10 years. Compared to other studies, including one by Blue Cross/Blue Shield, this is a very conservative estimate. Regardless of the actual total, it is clear that we're seeing billions of dollars funneled toward regulatory compliance at a time when health care providers are coping with dire fiscal austerity.

The Inova Health System in Virginia, with five hospitals and 1,400 beds, told a congressional staff briefing that their implementation costs had thus far totaled about $1.5 million. Concentra, a network of 244 occupational health care centers, has already spent $3 million on initial implementation of the Privacy Rule.

A single small hospital, Emerson Hospital of Concord, MA, has had to devote two full-time employees whose sole jobs will consist of HIPAA related paperwork. They will be compiling detailed information disclosure records that few if any patients will ever request.

There is a need to undertake a comprehensive review of these regulations to determine how to best achieve their intent, without forcing the expenditure of precious resources for nonessential compliance activities.

Mr. Chairman, health care companies and institutions want to act as working partners with the public and with the government to ensure that we achieve strong patient privacy protections without impeding treatment and medical research. While we still believe that the best course of action is a single, uniform Federal privacy standard, we look forward to working with this committee and with the Administration to ensure that Federal patient privacy protections serve the national interest as efficiently and effectively as possible.

Thank you.

[The prepared statement of Ms. Grealy follows:]

Testimony of

Mary R. Grealy
President
Healthcare Leadership Council

Hearing on

"HIPAA Medical Privacy and Transaction Rules: Overkill or Overdue?"

United States Senate Special Committee on Aging

September 23, 2003

Mr. Chairman, members of the Committee, thank you very much for this opportunity to testify on the issue of regulatory implementation of the Health Insurance Portability and Accountability Act (HIPAA). This is a matter of significant importance to America's patients, health care consumers and health care providers, and I appreciate being able to present the viewpoint of the Healthcare Leadership Council.

The Healthcare Leadership Council is a coalition of the chief executive officers of the nation's leading health care companies and institutions. The HLC membership embodies all sectors of health care – hospitals, health plans, pharmaceutical companies, medical device manufacturers, biotech firms, health product distributors, pharmacies and medical teaching colleges. Each and every one of our members is directly affected by the HIPAA privacy rule and, thus, HLC was and continues to be very involved in the development and implementation of the regulation.

The HLC also leads a coalition of over 100 organizations that strongly supports effective patient privacy protections. In fact, this coalition has supported legislation establishing national uniform privacy protections for health consumers. When the responsibility fell upon HHS, however, to put confidentiality protections in place, the coalition turned its efforts toward the development of a workable privacy regulation.

Before we discuss issues regarding the implementation of the HIPAA privacy rules – and there are significant issues that require attention – I want to spend a moment offering a broad review of the development and value of the regulation.

When it comes to this subject of patient privacy, every HLC member, every sector of the health care industry, has had the same concern and objective. How do we protect the sanctity of a patient's medical information privacy while, at the same time, ensuring that necessary information is available for providing quality

health care and conducting vital medical research? As well, how do you create effective confidentiality safeguards that do not burden providers and patients with unnecessary paperwork or delays in treatment?

We have the utmost respect for the officials in both the Clinton and Bush Administrations who wrestled with these issues and who diligently pursued a course that led us to the regulations we have today.

These regulations as revised by the current administration, while not perfect, do attempt to strike a balance between concerns about protecting personally identifiable medical information and the needed flow of information for treatment and research. Allow me to make four essential points about the value of these rules.

First, these regulations do exactly what they are intended to do. Disclosing identifiable health information for purposes other than carefully defined appropriate health care activities is prohibited unless the patient grants specific, prior written authorization. If you use a patient's medical record, without permission, for reasons other than legitimate health care purposes, you're going to be hit with federal civil and criminal penalties.

Second, patients are empowered by the modifications made by the Bush Administration in finalizing these rules. As now written, patients must be told how their information will be used and what rights they have to control their own data. This is an important step in giving patients greater control over their own personal information. We have always believed strongly, as well, that patients must have the right to review and amend their own records.

Third – and this is an important point when it comes to marketing – under the rules developed by HHS, patients will not receive marketing communications unless they actively opt in, unless they give their prior authorization. This is an

improvement over the original version of the rules, promulgated in the Clinton Administration, in which patients would have had to actively opt out of so-called marketing communications.

Fourth, and finally, these rules strike a vital and necessary balance when it comes to medical research. They maintain the "de-identification" of records in order to protect privacy, but give researchers access to information such as the patient's zip code or date of hospital admission. This information can be absolutely critical in tracing the outbreak of a disease. This is particularly important in light of our current bioterrorism threats.

Many potential difficulties in implementation were avoided when the regulations were revised last year. Under the Clinton regulations, patients would have had to give their written consent before they could receive treatment, receive a reminder to make an appointment, have your doctor schedule your surgery, or have a relative pick up a prescription for you. If these rules had not been revised, the more than three billion prescriptions filled last year and the hundreds of millions of hospital admissions and physician office visits would have been made more complex with unnecessary paperwork.

Even with these improvements, though, early implementation of the HIPAA regulations has clearly demonstrated that additional modifications are necessary. The rules' authors were wise to include a provision for the regulations to be revisited annually, to ensure that they are accomplishing their purpose without having unforeseen negative impacts on patients or providers.

As we look at possible modifications, we need to do so through the prism of quality patient care. Are any aspects of these regulations unnecessarily sapping resources, financial and human, from health care providers, resources that might otherwise be devoted to treating patients and pursuing improvements in health care quality?

Certainly, the price tag for implementing these regulations is a high one. The Department of Health and Human Services has estimated that the privacy rule will cost the private sector $17.5 billion over ten years. A study by Blue Cross Blue Shield – a member of HLC's confidentiality coalition – has placed the total costs even higher, stating that the total dollars spent on implementation, industry-wide, will be closer to $43 billion over five years. The important point here is that, regardless of whether implementation costs are $17.5 billion over ten, $43 billion over five or somewhere in-between, we're still seeing billions of dollars funneled toward regulatory compliance at a time when health providers are coping with fiscal austerity.

In fact, at a congressional briefing sponsored by HLC, just one health system – consisting of five hospitals and 1,400 beds – said their implementation costs had, thus far, totaled about $1.5 million. Extrapolate that total to the nation's health care system as a whole and it is easy to see that hospitals as well as all other health care providers are having to devote extremely large sums from their tight budgets in order to comply with HIPAA privacy rules.

In fact, wherever you look within the nation's health care system, you see entities having to carve dollars from limited revenues – dollars that could otherwise be devoted to patient care – to meet regulatory requirements.

- Marshfield Clinic, based in Wisconsin, analyzed the impact of just one small portion of the rule – the privacy notice requirement. The 660-physician group practice spent $75,000 – a cost that will continue to grow as new patients are added – to print, translate, sort and mail 200,000 privacy notices, as required by the rule.

- Concentra, a network of 244 occupational health care centers, spent $3 million on initial implementation of the privacy rule, including outlays

for consulting services, training costs, printing and other implementation activities.

- The National Association of Healthcare Access Management (NAHAM), a member of HLC's confidentiality coalition, is an association of organizations that provide oversight to patients and families as they enter the hospital system. NAHAM reports that the privacy rule is complicating existing processes that already meet the confidentiality needs of patients and that the regulations are adding a significant financial burden to an already taxed health care delivery system.

- Nursing homes, as well, are trying to find space within extremely tight budgets to comply with the HIPAA regulations. The American Health Care Association reported that it has spent nearly $1 million to provide educational materials on the rules to its nursing home members, and that is just a fraction of the compliance costs absorbed by the nursing home industry as a whole.

Clearly, it is necessary to undertake a comprehensive review of the regulations to determine how best to achieve the intent of the rules without forcing the expenditure of precious resources for non-essential compliance activities.

The American Hospital Association, also a member of the confidentiality coalition, has suggested, for example, that provisions regarding accounting for disclosures should be reviewed. Right now, the rule requires all covered entities to track the disclosure of patient health information (PHI) and maintain records on all patients – records that can be used to supply reports and disclosure statements on demand. At any time, an individual can request an accounting of PHI disclosures made by a covered entity for specific purposes. Individuals can request an accounting of all disclosures made over a six-year period.

What does this provision mean in practical terms? Let's look at the impact on just one hospital, Emerson Hospital in Concord, Massachusetts, a 145-bed community facility. Emerson will be required to document over 300,000 disclosures of protected health information each year. Let's assume that the tracking and recording of each disclosure takes one minute. That's 300,000 minutes, or 5,000 hours, per year – just to document disclosures in one community hospital. Again, extrapolate that to the nation's health system as a whole and you can understand the huge impact being felt by just one provision in these regulations.

At Emerson Hospital, compliance with this requirement means the hiring of two full-time employees whose sole jobs will consist of HIPAA-related paperwork. Assuming the average cost, in salary and benefits, for a clerical employee in Massachusetts, this will cost Emerson approximately $70,000 annually for regulatory compliance that provides only minimal patient benefits.

It is safe to say that only a very small percentage of patients will ask for a list of disclosure accountings after their care. Yet, under the privacy rule, Emerson must maintain a specific record of each disclosure in case a former patient should happen to request an accounting of all routine disclosures.

The American Hospital Association has provided to HHS a suggested change in this provision. Covered entities would develop a standard list of routine PHI disclosures that could be given to each patient who requests an accounting. This list would include, for example, the routine disclosures that are made for public health purposes – records of births and deaths, for instance. Covered entities would then only have to track non-routine disclosures for more detailed accounting reports. These non-routine disclosures would include those done, for example, for law enforcement reasons or to report suspected abuse.

As I said earlier in my testimony, constructing effective patient privacy regulations is, to say the least, a complex undertaking. Our most important challenge at this point is to make implementation of the rules as simple and meaningful as possible. Because of the regulations' complexity, we hope that the Office for Civil Rights responsible for its enforcement will take a real-world, common-sense approach. So far, we have every indication that they will.

This is particularly important in light of the fact that confusion still exists in various quarters on the rule's scope and implementation. Many companies in the medical device industry, for example, are not covered entities but have been asked by their hospital and physician customers to sign business associate agreements. Thus, they are affected by the HIPAA rule. Yet, there is considerable confusion and a lack of official guidance on the interaction between FDA regulations, international device standards, disclosures to foreign notified bodies for compliance purposes, and the HIPAA privacy rule.

It is essential that we never view these rules as a finished product, but rather as a meaningful regulation that must evolve and adapt with our constantly changing health care system.

We are doing our part at HLC, working with the confidentiality coalition, to assist entities with regulatory compliance. We have funded a million-dollar study that compares the new federal privacy regulations with existing state laws, so that providers and their business associates will know if they must comply with the state law, the federal rules or both. We are serious about compliance and helping hospitals, physicians, health plans and others with that effort. It should be noted, though, that as we illustrate this patchwork quilt of federal regulations and varying state laws, it further underscores the need for a single federal privacy standard affecting all patients and all health care entities uniformly.

Health plans and providers want to act as working partners with the public and with the government to ensure that people feel secure in their privacy, while at the same time making sure that we don't impede their treatment and research that will bring better health care in the future.

The good news is that this rule can be revised annually, so that the public will have the opportunity to seek necessary revisions. We look forward to working with this committee and with the Administration to ensure that federal patient privacy regulations serve the national interest as efficiently and effectively as possible. Thank you.

The CHAIRMAN. Thank you, Miss Grealy.

We will next hear from Miss Fox.

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

Ms. FOX. Thank you, Mr. Chairman. I appreciate the opportunity to testify this morning on HIPAA's administrative simplification rules.

Blue Cross Blue Shield plans across the country are very committed to the goals of administrative simplification to reduce the costs, hassles, and paperwork of our health care system. However, we are concerned that these goals will not be realized unless we change the entire process for establishing and implementing the many administrative simplification standards that lie ahead of us.

I would like to make three points. First, despite a 3-year implementation period, with an extra year that we got, thanks to your leadership, Mr. Chairman, we still have many providers who are not ready for the October 16 HIPAA transaction and code set regulation, just 3 weeks away. As a result, payers are planning to deploy expensive backup contingency arrangements to minimize disruptions and prevent unintended consequences, such as providers returning to paper in order to get paid.

There are several reasons for our unreadiness: general lack of awareness about the regulation, especially among small and rural providers; lack of understanding about the cost and complexity of what it takes to become HIPAA compliant; and the late revisions made to the rule just last February that resulted in delayed vendor software needed by the industry.

Second, important lessons can and should be learned from the first phase of HIPAA administrative simplification which should be considered before additional standards are adopted.

It is important to realize there are numerous additional standards on the horizon. They fall into three categories. There are additional HIPAA rules that HHS is expected to release in the next year that Cathy Treadway talked about a little bit earlier. Second, there are modifications to the standards that we are just now implementing, some of which call for wholesale, very expensive changes, such as ICD–10, and new information technology initiatives by Congress and the administration to develop uniform standards for clinical information and the interoperability of information systems so that patients' medical records can move from doctor to doctor across the country electronically.

We believe the lessons learned include, first, a credible cost-benefit analysis, which is a must before any future standards are adopted. When HHS adopted the transaction and code set rule, the projected costs were greatly underestimated. HHS estimated the cost at $5 billion for the entire industry. Two years ago, we commissioned the Nolan Company who found the HHS estimate to be understated by a factor of 10 for health plans and a factor of 3 for providers, thereby underestimating total industry cost by $11 billion.

Now that the compliance date is here, it appears the Nolan estimate is on the low side and that the actual industry costs just to implement the HIPAA administrative simplification transaction

and code set rule are likely to be significantly higher than the earlier $16 billion we originally estimated.

A second lesson learned is that the industry must involve all aspects of their operation in developing the standard, not just the IT shop. A key mistake all stakeholders made is treating administrative simplification as a systems issue, just like Y2K. We have found, however, that these standards have a ripple effect throughout the entire health care operation, whether it's a payer, a health care clinic, or a hospital. A change in one simple code can affect medical policy, quality improvement programs, how much you get paid for the service, as well as fraud and abuse detection efforts, just to name a few.

The third lesson is standards must be pilot-tested before we adopt them. It is only when a standard is actually pilot-tested that we can identify the issues and any unintended consequences that should be addressed before we ask the entire industry to go ahead and adopt them.

Finally, we urge Congress to create a high level stakeholder commission to develop a national health care information technology strategy based on industry consensus. The current piecemeal approach to information standards is akin to building a house room by room without an overall blueprint. While the standards now being contemplated have great potential to improve quality and cut costs, this goal will not be realized under the current process. The industry needs a blueprint to know where we are headed, with a prioritization and timeline to provide order and predictability to all of us, and importantly, to ensure that the standards are implemented in the most cost-effective and efficient manner.

Mr. Chairman, as you have highlighted this morning, with so many demands on the industry, health care premiums rising at double digit rates, and with over 40 million Americans uninsured, it is critical that we spend our resources wisely.

Thank you.

[The prepared statement of Ms. Fox follows:]

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans

1310 G Street, N.W.
Washington, D.C. 20005
202.626.4780
Fax 202.626.4833

TESTIMONY

Before the

Special Committee on Aging
United States Senate

on

Regulatory Implementation Repercussions Stemming from the Health Insurance Portability and Accountability Act (HIPAA)

Presented by:

Alissa Fox
Executive Director, Policy

September 23, 2003

Mr. Chairman, I am Alissa Fox, Executive Director, Policy for the Blue Cross and Blue Shield Association (BCBSA). I appreciate the opportunity to testify today on administrative simplification implementation issues. BCBSA represents 42 independent Blue Cross and Blue Shield Plans (Plans) across the country that together provide health coverage to almost 89 million people, one in three Americans.

BCBS Plans are committed to the goals of administrative simplification: reduce administrative costs and complexities of the health care system in order to minimize hassles and paperwork for providers.

My testimony focuses primarily on the HIPAA Transactions and Code Sets Regulations (T&CS) and covers six areas:

1. The current state of industry readiness is extremely low to meet the October 16, 2003 compliance date for the HIPAA transactions and code sets regulation (T&CS), requiring payers to deploy "back up" contingency arrangements.
2. BCBSA is concerned that some entities are attempting to unravel the standards and circumvent the established process for obtaining changes to HIPAA standards by seeking HHS guidance contrary to the intent of the law.
3. BCBSA and its member Plan's have worked to provide industry leadership and provider outreach throughout the T&CS implementation period.
4. Important lessons can be learned from implementing the initial HIPAA standards which should be considered before additional standards are adopted.

5. Policymakers are now advocating the next phase of national health care information standards -- "HIPAA II" -- for clinical information and interoperability of health care systems. These initiatives are proceeding in an uncoordinated, piecemeal and inefficient fashion, which will increase spending and waste industry resources.
6. The creation of a high-level stakeholder commission is urgently needed to develop a national health care information technology strategy based on industry consensus.

Background

The Health Insurance Portability and Accountability Act (HIPAA) was enacted into law in 1996. The administrative simplification provisions of HIPAA required the Department of Health and Human Services (HHS) to adopt standards in the following areas: healthcare transactions and code sets; privacy of individually identifiable health information; security of health care information; and national identifiers for providers, employers and health plans. The law provides a 24-month implementation period after each regulation is adopted before health plans, clearinghouses, and providers that electronically transmit health care information must comply with the law.

On August 17, 2000, the Department of Health and Human Services issued final rules for the standardization of the form and content of the following electronic healthcare transactions:

- Claims and encounter transactions;
- Coordination of benefits;
- Enrollment and disenrollment;
- Eligibility inquiries and responses;
- Payment and remittance advice;
- Premium payments;
- Claims status inquires and responses;
- Referral authorizations; and
- Retail pharmacy.

In addition to transaction formats, the rule also requires the use of certain code sets within the transaction – both clinical codes (i.e., ICD-9, CPT-4) and transaction codes (i.e., gender, relationship of patient to subscriber). Covered entities were originally required to be compliant by October 16, 2002.

However, in December of 2001, the Administrative Simplification Compliance Act (ASCA), provided a 12-month extension of the transactions and code sets deadline. To help ensure compliance, the bill required covered entities to file a "compliance extension plan' with HHS by October 2002. The law also requires all but very small providers and those exempted by the Secretary of HHS to file claims electronically with Medicare by

October 16, 2003. Drafters of the legislation believed that this would improve industry compliance and encourage covered entities to better understand the requirements and tasks needed to come into compliance one year in advance of the new deadline.

Four of the seven initial HIPAA rules have been finalized. HHS is expected to issue additional HIPAA rules over the next year, including a final rule for the national provider identifier and proposed rules for national health plan identifiers and the claims attachment transaction. HHS is also expected to publish a second modification to the transaction and code set rule in Spring 2004. In addition, HIPAA gives HHS discretion to adopt additional financial and administrative transactions – beyond the initial HIPAA rules -- to promote efficiency in the healthcare system.

I. Current state of industry readiness is extremely low to meet the October 16, 2003 compliance date for HIPAA transactions and code sets rule, requiring payers to deploy contingency arrangements.

In July, HHS issued enforcement guidance that allows health plans to accept non-standard transactions, in addition to fully HIPAA compliant transactions, during an interim period as part of a good faith compliance effort. These "contingency plans" are necessary because a significant number of providers and plan trading partners will not be ready to meet the October 16 compliance date for the transactions and code sets rules. Under HIPAA, payers can only accept fully HIPAA compliant electronic claims or paper claims. We are pleased that the recently issued HHS guidance will allow payers to accept

existing formats during an interim period if they can demonstrate "good faith compliance." This will prevent cash flow disruptions for providers.

For many plans, operating dual systems – existing and HIPAA compliant systems – will further increase the cost and administrative burden of the HIPAA regulations. In 2001, the Robert E. Nolan Company (Nolan) issued a report commissioned by BCBSA that projected the cost of HIPAA transactions and code sets for health plans, hospitals and physicians to be $16 billion. While we have not re-estimated those costs at this time, the Nolan projection for large health plans spending-- $10 million--, appears to be on the low side and therefore the actual industry costs is likely to be significantly higher than the earlier $16 billion estimate. In fact, many Plans have indicated that the cost of transactions and code set regulations have equaled the amount spent on Y2K.

Before HIPAA, Blue Cross Blue Shield plans were already highly automated. Approximately, 90 percent of hospital claims and 60 percent of physician claims were submitted and adjudicated electronically. A substantial increase in paper transactions will dramatically increase costs and resources for HIPAA implementation. One plan has estimated it costs $2.00 more per claim to process paper vs. electronic claims. Another plan has reported an increase in paper transactions already. Worse yet, some of these paper claims are hand written and therefore unable to be electronically scanned for input into adjudication systems.

Provider readiness has been slowed by lack of awareness and considerable misinformation about the ability of vendors and clearinghouses to make providers compliant coupled with the fact that many clearinghouses and vendors will not reach compliance by the deadline. A spring Healthcare Information and Management Systems Society/Phoenix Health Systems (HIMSS/PHSS) indicated that just 50 to 60 percent of clearinghouses and vendors are likely to be ready to accept/transmit HIPAA-compliant transactions by the October 2003 deadline.

According to the HIMSS/PHSS survey, respondents stated that "not enough time" was the primary roadblock to HIPAA compliance. Two years ago, BCBSA took an active, leadership position advocating for an extension of the original October 2002 compliance date because of the cost and complexity of the rule and the lack of provider and vendor readiness to meet the compliance deadline. The extension was also important because it provided needed time for HHS to publish, and the industry to adopt, the 4010A1 version of the standard, which was necessary to avoid serious operational issues posed by the original version (4010).

II. BCBSA and member Plans are committed to HIPAA administrative simplification and its national uniform standards, however, we are concerned that some entities are attempting to unravel the standards and circumvent the established process for obtaining changes to HIPAA standards by seeking HHS guidance contrary to the intent of the law.

Many organizations greatly underestimated the cost and complexity of the HIPAA transactions and code sets rule. Ironically, some of the very organizations that opposed the legislation to extend the compliance date back in 2001 because they were "ready" have told Plans now that they are not compliant. Some other entities have presented arguments to HHS that health plans must accept and process claims without all the data requirements mandated by HIPAA. These arguments are being advanced because some health care providers cannot produce the required data necessary to transmit a HIPAA compliant electronic claim by the October deadline. These organizations want HHS to "clarify" that payers should be required to accept claims with just a subset of the HIPAA required data. These eleventh hour attempts to change the intent and objectives of HIPAA will undermine the law and defeat the purpose of national uniform standards. The result will only serve to punish the entities that have spent the time and money to meet the requirements of HIPAA in accordance with the regulations and HHS guidance. To allow providers to submit, and require health plans to accept, transactions without all required HIPAA data is unworkable for many payers.

Payers have invested extensive dollars and human resources to be fully compliant by October 2003 as required by law. To implement partial compliance would require additional staff effort and expense and would require months of systems rework. Many Plans believe they would have to build and maintain a second system, thereby running three systems (one for fully compliant submitters, one for partially compliant submitters, one for those submitters using existing formats.) Allowing providers to submit claims

without all HIPAA required data will lead us right back to the current environment – different data requirements for every health plan.

HIPAA provides a process by which any individual or entity may request a change to the transactions through designated standards maintenance organizations. We believe that this process must be followed and any attempt to change the standard through "guidance" should be opposed.

III. BCBSA and its member Plan's have worked to provide industry leadership and provider outreach throughout the T&CS implementation period.

Plans have been involved in extensive provider outreach programs designed to help their trading partners better understand both the requirements and the tasks required to reach compliance. The following highlights these actions:

- In May 2003, the Association announced the introduction of a ***HIPAA Transaction and Code Sets Toolkit.*** The toolkit was designed as a resource for professional providers in order to better understand the new HIPAA transactions and code requirements and promote compliance. The document was commissioned by BCBSA and written by Margaret Amatoyakulmake with Boundary Information Group. BCBSA sent the document to all member Plans to make available to their providers at no cost. The toolkit is available on the BCBSA website as well as those of our member Plans. Several provider associations are linking their website to our website to make the document available to their members.

- In 2001, BCBSA released a document entitled "HIPAA's Myths, Practical Realities and Opportunities: The Work Providers Need to Perform For Standard Transactions and Code Sets." The document was commissioned by BCBSA and produced by PricewaterhouseCoopers to dispel some of the popular myths circulating about HIPAA and shed light on the scope and magnitude of the effort providers will need to undertake to achieve compliance.
- BCBSA also worked with Tillinghast-Towers Perrin to produce a report entitled "Provider Cost of Complying and Standardized Electronic Formats" which estimated costs for providers to reach compliance with the Transactions and Code Sets regulations. We believed that without a clear understanding of projected expenditures, covered entities would not budget sufficient financial and administrative resources to meet the requirements of HIPAA by the deadline.
- BCBSA also developed a document for providers identifying the HIPAA Contract for each member Plan. This is also available on our website and we have made it available to numerous provider associations to post to their websites as well.
- In addition to BCBSA outreach programs, our individual Plans have implemented numerous HIPAA education and awareness programs for providers. These include conferences and workshops, dedicated provider mailings on HIPAA and individual phone calls with key electronic submitters. They have also dedicated staff and resources to industry coalition efforts. BCBSA and Plans continue to be very active and maintain leadership positions with both local and national organizations related to HIPAA such as WEDI and WEDI SNIP. We are active participants in terms of

identifying, addressing, and resolving industry issues, problems and concerns related to implementation.

IV. Important lessons can be learned from implementing the initial HIPAA standards, which should be considered before additional standards are adopted.

Before any additional standards are developed and adopted, the industry should evaluate the implementation of the HIPAA regulations to date and identify ways to improve the standards process.

Over the past several years, our member Plans have identified several "lessons learned" from implementing the initial HIPAA transactions and code sets standards. The following is a brief list of issues to be considered before future national healthcare standards are adopted.

- **Credible cost/benefit and industry impact analysis is required before standards are adopted.** When HHS adopted the transactions and code sets rule, the projected industry costs were greatly underestimated and savings were overstated. According to HHS analysis, a large health plan would spend approximately $1 million implementing the standard and a large hospital (100 plus beds) would spend $250,000. Consequently, entities underestimated the resources need to comply with the standard and inadequately budgeted. There were no cost estimates for Medicare or Medicaid, yet Medicaid spending alone was expected to exceed $1 billion

according to an earlier estimated by the American Public Human Services Association (Association of Medicaid Directors).

- **Standards must be pilot tested before adoption.** One of the main reasons that many entities are not ready to meet the October TCS compliance date is because the industry had to wait for the publication of a critical modification to the original rule. The modification was not published until February of this year and many vendors refused to remediate their software until the final rule was published. This left little time to rework systems and test with trading partners. It also increased unnecessary spending. Much of this could have been avoided if the original standard was pilot tested and the deficiencies or needed changes were identified and incorporated before national implementation began.

- **A concerted national education campaign is critical to the successful implementation of mandated, uniform industry standards**. Many covered entities, particularly small and rural providers still do not fully understand the requirements of T&CS. The success of administrative simplification is contingent upon all covered entities being able to send and receive HIPAA compliant transactions. An education plan is also important to dispel misconceptions about the standards. For example, many providers believed that a vendor or clearinghouse could make a covered entity HIPAA compliant. In the 2001 PWC report entitled *HIPAA's Myths Practical Realities and Opportunities: The Work Providers Need To Perform For Standard Transactions and Code Se*ts, it states:

> "regardless of whether a provider uses a clearinghouse or vendor, the provider will still need to perform a significant amount of the work, including assessing and changing business processes to collect and submit much more data than today, training staff on the new codes and modifying business operations to address the "ripple" effect of systems changes. . . This type of misinformation dissuades providers from doing the necessary analyses to identify needed operational and contractual changes to be compliant with HIPAA T&CS."

While BCBSA widely distributed the PWC report, many providers are still unaware.

V. "HIPAA II" – standards for clinical information and interoperability of health care systems – is proceeding in an uncoordinated, piecemeal and inefficient fashion, which will increase spending and waste industry resources.

Over the past year, there has been a proliferation of information technology initiatives by Congress and the Administration to develop national uniform standards for clinical information and the interoperability of information systems. There are many benefits that can be achieved through these proposals: reducing medical errors, improving quality, lowering health care costs and improving public health. These proposals are being pursued in addition to the numerous HIPAA financial and administrative standards the industry is currently implementing and the three pending HIPAA regulations that HHS is expected to release within the next year.

While we are very supportive of the objectives of these initiatives, these new clinical information standards are being advocated without a national strategy, prioritization or industry consensus on the direction and timeline for these standards. As evident by the ongoing issues the industry is struggling with regarding the implementation of HIPAA T&CS, an orderly and well defined strategy is essential to a cost effective and efficient implementation of standards. These initiatives and proposals include:

- **S.1/H.R.1 Prescription Drug and Medicare Improvement Act**. A provision in the bill would require HHS to establish national standards for electronic Rx prescribing. The system envisioned would electronically connect pharmacies, doctor's offices, and health plans in real time. These systems do not exist today as envisioned by the legislation and very ambitious timelines are being contemplated.

- **H.R. 663./S.720 – Patient Safety and Quality Improvement Act**. The bill would require HHS to develop voluntary national standards for the "interoperability" of information technology systems (so the entire health care industry's computers can talk to each other in real time). Neither "interoperability" nor "health care information systems" are defined but encompass a wide range of possibilities.

- **Consolidated Health Informatics** – This Administration initiative is part of the President's e-Gov initiative. The project's goal is to adopt a portfolio of 24 data and messaging standards for the interoperability of health information among federal

agencies. These standards are needed to make electronic medical records interoperable.

- **National Health Information Infrastructure (NHII) --** This HHS initiative is to create public/private interoperable systems for electronic health records, personal health records and public health reporting.

- **ICD-10** – The National Committee on Vital and Health Statistics (NCVHS) is currently considering a recommendation to the Secretary to adopt ICD-10 CM/PCS to replace ICD-9 for diagnosis and inpatient procedure codes. It is expected that the committee will adopt a recommendation this November. Last September, BCBSA, together with American Association of Health Plans, the Health Insurance Association of America, the National Association of Medicaid Directors and the Joint Committee on Accreditation of Healthcare Organizations urged the committee to commission a cost/benefit analysis before adopting a recommendation. A report by Rand is expected to be released this week. BCBSA also commissioned Nolan to perform a cost/benefit analysis. While Nolan is only prepared to discuss preliminary results at a NCVHS hearing this afternoon, it will state that costs for hospitals, physicians, and payers are projected to be as high as $14 billion. A final report will be released in October. Nolan is still receiving stakeholder survey data that could impact these cost estimates, particularly the cost to government programs and regional hospitals. Interestingly, the report also raises the question as to the appropriate sequence of standard adoption. For example, the author argues that in

order for any benefits from ICD-10 CM/PCS to be achieved, standardization of a clinical vocabulary is a prerequisite. While this assertion needs to be validated and the impact of a national standard for clinical vocabulary analyzed, it does call into question our national strategy, or lack thereof, for information healthcare technology.

VI. The creation of a high-level stakeholder commission is urgently needed to develop a national health care information technology strategy based on industry consensus.

The current piecemeal approach to national healthcare information standards is like building a house room by room without an overall blueprint. The health care industry needs a national healthcare information technology blueprint to provide order and predictability to stakeholders and to ensure that standards are implemented in the most cost effective and efficient manner.

This blueprint should consider the consequences of the continuing demand on industry resources needed to implement the multitude of standards contemplated. While there is no comprehensive industry cost estimates of implementing Privacy and Transactions and Code Sets, it seems clear that current costs are in the tens of billions of dollars.

BCBSA recommends the creation of a stakeholder commission to reach a consensus on the goals and objectives of a national information infrastructure and to develop a comprehensive strategy for the adoption and implementation of voluntary standards. The

Commission would report back to the Congress with its recommendations on a timeline, and prioritization of standards taking into account the cost, benefit and feasibility of national implementation for each standard. Congress would then develop clearly defined legislation to implement the recommendations of the Commission. We believe that a commission is essential and urge the Congress to adopt this strategy before requiring HHS to develop additional health care information standards.

Thank you for the opportunity to speak to you on this important issue. I am pleased to answer any questions Members of the Committee may have.

The CHAIRMAN. Miss Fox, thank you very much.

Now, the last person on this panel, Janlori Goldman, Director of the Health Privacy Project. Welcome. We look forward to your testimony.

STATEMENT OF JANLORI GOLDMAN, DIRECTOR, THE HEALTH PRIVACY PROJECT

Ms. GOLDMAN. Thank you. Thanks very much for inviting me to testify.

As you probably know, the Health Privacy Project not only develops expertise and analysis on a range of health privacy issues, we also coordinate a consumer coalition for health privacy. It is made up of provider groups and disability rights groups, labor organizations and consumer groups so that we can better represent the interests of patients, since we all are patients. We can better represent the interests of patients who both want research to go forward, and want to improve health care, but also want to make sure they're not putting themselves at risk for discrimination and privacy violations.

The Privacy Rule, as you have heard already today, is the first Federal law that provides a minimum set of privacy and security rules for Medical information. It allows both provider groups and health plans to build privacy into the practice of delivering health care.

One of the things that has not been discussed this morning that I want to talk about for a moment is why we needed this health privacy law. We needed it because we had documented evidence that, without privacy, people had barriers to care, quality of care was at stake, and some people were afraid to get health care because they didn't want to subject themselves to potential discrimination. They were afraid their employers would get access to information, they were afraid that friends and family members, coworkers, might learn about sensitive conditions. Where they were not able to be honest with their doctors, they put themselves at risk for untreated and undiagnosed conditions.

We believe very strongly that there is a high cost that has been paid by the public because of the lack of privacy, and a cost that has not been assessed either by this Administration or by any of the industries who talk to you about the cost of putting privacy in place. We believe there will be substantial cost savings, not just the offset from the transaction and code set rules, but also because people will be more encouraged to fully participate in their own care and, again, not put themselves at risk.

We also know not just the empirical data in terms of this 20 percent who have withdrawn from care, but we also know individual stories that have been very compelling, people who have lost their jobs because information was misused, people whose information was sold without their permission, people whose information was put on the Internet, and most recently, even in the Kobe Bryant case, the accuser there had her medical records released by a hospital in Colorado without her knowledge, without her permission, and against both Colorado law and the privacy regulation.

The Privacy Rule, as you heard, was a long time in the making. It went through an extensive rulemaking process. The Bush Ad-

ministration did make substantial modifications to ease industry concerns. But we do have limits on access and disclosure outside of health care. People can now get their own records, and the notice is very substantial in telling people how their information is used.

Despite a 2½ year implementation process and compliance period, myths do persist. I think that Director Campanelli testified very eloquently about how most of those myths have been dispelled. Most of the initial myths and misperceptions and confusion about the privacy regulation was in some ways kind of a blip. There was a lot of early misunderstanding, most of which was put to rest by OCR, and by the industry. The Health Privacy Project put out a Know Your Rights. We have done some substantial public education.

But some of the myths do persist, and I think they're very troubling. For instance, the myth that doctors can't share information with each other or other health care providers—absolutely wrong. Relatives can visit their family members in the hospital and pick up prescriptions and other kinds of medical information unless, of course, the patient has taken a step to opt out.

The notice is not a consent form. The Bush Administration was clear that consent is not required for treatment and payment. The notice tells people how their information is used and what their rights are. It does not have to be signed. We just encourage people to do it to acknowledge that they received it. There is no private right of action, so under the Federal law people don't have a right to sue.

The cost issue I think I have addressed already.

State law, which some people have addressed, is really important. Prior to promulgation of the privacy law, the Health Privacy Project compiled and summarized State Medicaid privacy laws. They are available on our website for free.

We found that the Privacy Rule will bring substantial uniformity. Yes, there will still be 50 different State laws, but for the most part, most of them will be preempted because the Federal rule is more stringent or more comprehensive. Where the State laws will still continue to exist is usually in a condition-specific area. There are specific laws related to HIV/AIDS or mental health, or abuse and neglect. Those laws were carefully crafted at the State level and they will continue to stand. The Privacy Rule doesn't address medical privacy on a condition-specific basis.

Let me just conclude with three quick points. We believe the privacy regulation is absolutely important in encouraging people to get care, in improving quality of care, so the information we have for research and public health is reliable. We believe that it allows information to flow freely within the health care context without barriers, but it puts limits and safeguards in place so the information will not go to employers, will not go to law enforcement without some court order, that there are some limits in place. We think that's critical.

The temporary confusion, as I have said, I think has been addressed by OCR, by the Health Privacy Project, and others. But I want to urge the professional and trade associations, many of whom are in this room today, to step up their technical assistance and their guidance. Some of the confusion that occurred early on

I think was inexcusable, involving some very fundamental, basic misunderstandings and confusion. So I think we know what those areas are and to step up technical assistance is key.

Again, I don't think it is fair to ask people to sacrifice their own health care and their own ability to get care in order to protect their privacy. We know a substantial portion of this population has done that so far. My hope is that, over the next few years, we will be able to go back into the public and do another survey following up on our 1999 survey, to measure if the privacy regulation encouraged people to get care. Has it encouraged doctors and patients to communicate more freely with each other? Have we seen that the cost issues in some ways are outweighed and maybe even offset by increased participation and by the transaction and code sets? So I look forward to that continuing dialog with you and the rest of the committee.

Thank you.

[The prepared statement of Ms. Goldman follows:]

Testimony of

Janlori Goldman, Director
Health Privacy Project

Before the
Senate Special Committee on Aging

Regarding Implementation of the HIPAA Privacy Regulation

September 23, 2003

To Committee Chairman Craig, Senator Breaux, and Members of the Committee:

On behalf of the Health Privacy Project, I am very appreciative for the opportunity to testify before you today on the medical privacy regulation mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The landmark privacy rule is the first comprehensive federal law aimed at safeguarding the confidentiality of patient records within the health care system. In mandating the law, Congress recognized that protecting patient privacy is central to fostering both access to health care and high quality health services. Since the April 14, 2003 date by which health care providers, plans, and others were required to comply with the law – following more than two years for implementation – there has been both confusion and misunderstanding about certain provisions of the law. Some of the confusion was anticipated, and could have been addressed through more rigorous guidance and education from regulators and professional associations. Nevertheless, many of the initial glitches have been resolved and clarified, and phone calls regarding implementation questions to both the HHS Office of Civil Rights (OCR) and the Health Privacy Project have decreased in the last couple of months. In addition, OCR's guidance over the past few months has grown increasingly comprehensive and targeted to the bulk of questions and concerns that have arisen.

However, where misinterpretation persists, we urge that both the HHS Office of Civil Rights, and the professional and trade associations representing providers, plans, and others affected by the law, aggressively step up their technical assistance and guidance. We believe that resources should be devoted to proper and vigorous implementation, and not to using misunderstanding and mishap to build public opposition to the law. Evidence of confusion must commit us to better educating the public, not to undermining support for the medical privacy protections the public clamored for decades. To better educate consumers in a simple, easy-to-read format, the Health Privacy Project published "Know Your Rights," which is available as a brochure and on our web site.

Halfway through the two year compliance period, a California HealthCare Foundation survey of health care organizations indicated that although implementation efforts were well underway, there were areas of confusion and misinterpretation. The health care industry and regulators were put on notice at that time that more resources were needed to ensure the law was better understood. At this stage, we urge Congress to request that a follow-up study

be conducted, possibly by GAO or the NCVHS, that measures the status and impact of implementation.

Our testimony highlights the major myths about the privacy rule, and sets the record straight with the facts. Our testimony also addresses the cost of implementing the privacy rule, citing this administration's own findings that privacy costs will be significantly offset by savings achieved through standardizing transactions and code sets. Savings will also be achieved as people more fully participate in their own care, thereby reducing the risk of undiagnosed and untreated conditions. We also include here a brief overview of the history of HIPAA, and the urgent public need for a medical privacy law.

The Health Privacy Project

The Health Privacy Project is dedicated to broadening access to health care, and improving the quality of care by ensuring that people's medical information is safeguarded in the health care arena. The Project conducts research and analysis on a wide range of health privacy issues, including objective analysis of the new regulation, a compilation of state health privacy laws, genetics and workplace privacy, reports on e-health and health web sites, and an initiative on public health emergencies. In addition, the Health Privacy Project coordinates the Consumer Coalition for Health Privacy, comprised of over 100 major groups representing consumers, health care providers, and labor, disability rights, and disease groups. Coalition participants include AARP, the American Nurses Association, Bazelon Center for Mental Health Law, National Multiple Sclerosis Society, National Association of People with AIDS, National Organization for Rare Disorders (NORD), and the Genetic Alliance. A complete list of Coalition participants, as well as all of the Project's resources related to health privacy, can be found at our web site, www.healthprivacy.org.

Urgent Need for Health Privacy

Previously, the lack of a national health privacy law had a negative impact on health care, both on an individual as well as at the community level. A 1999 survey by the California Health Care Foundation documented that one out of every six people withdraws from full participation in their own care out of fear that their medical information will be used without their knowledge or permission. These privacy-protective behaviors include patients providing false or incomplete information to doctors, doctors inaccurately coding files or leaving certain things out of a patient's record, people paying out of pocket to

avoid a claim being submitted, or in the worst cases, people avoiding care altogether.

More specifically, a 1997 survey documenting people's fears about genetic discrimination showed that 63 percent of people would not take genetic tests if health insurers or employers could obtain the results. (*Genetic Information and the Workplace,* issued on January 20, 1998 by the U.S. Departments of Labor, Health and Human Services, and Justice, and the U.S. Equal Employment Opportunity Commission). And, a study involving genetic counselors documents that fear of discrimination is a significant factor affecting willingness to undergo testing and to seek reimbursement from health insurers. (Hall, Mark A. and Stephen S. Rich, *Genetic Privacy Laws and Patients' Fear of Discrimination by Health Insurers: The View from Genetic Counselors*, 28 Journal of Law, Medicine & Ethics 245-57 (2000).)

An April 2001 Harris survey documents that nearly four out of ten (40%) people with multiple sclerosis said they have lied or failed to disclose their diagnosis to colleagues, co-workers, friends or even family members out of fear of job loss and stigma.

These survey figures come to life in the daily media reports of people being harmed by the inappropriate use of their health information. To highlight just a few:

- Just recently, the alleged victim in the Kobe Bryant rape case had her medical records regarding a previous hospitalization released by hospital staff, who it appears violated the HIPAA privacy regulation. The hospital's own motion following the unauthorized disclosure argues that the records were shared in violation of the rule, and requests that they be returned to the hospital or destroyed.

- The medical records of an Illinois woman were posted on the Internet without her knowledge or consent a few days after she was treated at St. Elizabeth's Medical Center following complications from an abortion at the Hope Clinic for Women. The woman has sued the hospital, alleging St. Elizabeth's released her medical records without her authorization to anti-abortion activists, who then posted the records online along with a photograph they had taken of her being transferred from the clinic to the hospital.

- Terri Seargent was fired from her job in North Carolina after being diagnosed with a genetic disorder that required expensive treatment. Three weeks before being fired, Terri was given a positive review and a raise. As such, she suspected that her employer, who is self-insured, found out about her condition, and fired her to avoid paying costly medical expenses.

- Several thousand patient records at the University of Michigan Medical Center inadvertently lingered on public Internet sites for two months. The problem was discovered when a student searching for information about a doctor was linked to files containing private patient records with numbers, job status, treatment for medical conditions and other data.

- Joan Kelly, an employee of Motorola, was automatically enrolled in a "depression program" by her employer after a prescription drugs management company reported that she was taking anti-depressants.

- The Florida Attorney General's office investigated the marketing practices of Eckerd Drug Company to determine whether or not the company violated customers' privacy. When customers picked up their prescriptions, the chain drug compnay had them sign a form not only acknowledging receipt of a prescription but also authorizing the store to release their prescription information for future marketing purposes. The form apparently did not adequately inform customers that they were authorizing the commercial use of their medical information. According to the Attorney General's investigation, no customer or store employee interviewed was aware of the fact that the customer had actually signed an authorization for marketing purposes. As part of a settlement, Eckerd agreed to change its policies to better protect patient privacy, including restricting the direct marketing of prescription drugs to customers who have given written consent to use their medical information for such purposes. The company also agreed to fund a $1 million ethics chair at the Florida A & M School of Pharmacy.

- Eli Lilly and Co. inadvertently revealed 600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac. In the past, the e-mail messages were addressed to individuals. The message announcing the end of the reminder service, however, was addressed to all of the participants.

- Last year, 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.

In the absence of a federal health privacy law, these people suffered job loss, loss of dignity, discrimination, and stigma. Had they acted on their fears and withdrawn from full participation in their own care – as many people do to protect their privacy – they would have put themselves at risk for undiagnosed and untreated conditions. In the absence of a law, people have been forced to choose between shielding themselves from discrimination, or receiving health care services.

The Genesis of the Privacy Rule

The HIPAA Privacy Rule is a major victory for all health care consumers, and takes a significant step toward restoring public trust and confidence in our nation's health care system. The regulation fills the most troubling gap in federal privacy law, setting in place an essential framework and baseline on which to build. Each one of us stands to benefit from the Privacy Rule in critical ways, including greater participation in the health care system, improved diagnosis and treatment, more reliable data for research and outcomes analysis, and greater uniformity and certainty for health care institutions as they develop privacy safeguards and modernize their information systems.

Most notably, the Privacy Rule requires health care providers to give people notice of their rights under the new law and to inform people about how their health information will be used; grants people the right to see and copy their own medical records; imposes limits on disclosing patient records to employers; broadens the scope of protection for people whose health information is used by privately-funded researchers; puts safeguards in place for disclosure to law enforcement; and allows for civil and criminal penalties to be imposed if the Rule is violated.

The Privacy Rule was issued by the Department in December 2000 in response to a mandate from Congress included in the 1996 Health Insurance Portability and Accountability Act (HIPAA), which required that if Congress did not enact a medical privacy statute by August 1999, then HHS was required to promulgate regulations. Congress did miss the deadline, and after the mandate shifted to HHS, the rule was the subject of a lengthy, thorough, and robust rule-making process – both before and since it was released in December 2000.

Despite intense pressure from some in the health care industry, the Bush Administration allowed this important regulation to go into effect in April 2001. The first implementation guidance issued by the Department on July 6, 2001, addressed the many misstatements and exaggerations that some in the industry had spread about the Privacy Rule. That guidance– and much of the guidance that followed– appears aimed at calming industry fears, promoting clarity, and fostering compliance with the regulation.

When President Bush allowed the Privacy Rule to go into effect in April, 2001 he issued a strong statement about the need to protect patient privacy and foster confidence that people's "personal medical records will remain private." The President also pledged during his campaign to support a law requiring that a "company cannot use my information without my permission to do so," and expressed support for strong laws protecting medical and genetic privacy. In fact, William Safire dubbed him the "privacy President" in a New York Times column shortly after the Privacy Rule went into effect.

We believe that the Privacy Rule – as finalized – could go farther in protecting patients. One shortcoming is that the rule only directly regulates providers, plans and clearinghouses, and does not directly regulate employers, pharmaceutical companies, workers compensation insurers, and many researchers. Also, the regulation lacks a private right of action that would give people the right to sue if their privacy is violated. Under HIPAA, only Congress and the states are empowered to address these limits. Other weaknesses, such as allowing sensitive medical information to be used for marketing without patient knowledge or consent, are within the HHS' authority to regulate.

The history of the Privacy Rule's genesis is important here. Many in the health care industry pressed Congress to include in HIPAA the mandate for transaction and code set regulations to be developed (known pithily as "Administrative Simplification"). The industry's mission at that time was to put in place a common language for the coding of certain patient encounter data so as to streamline billing, and create greater efficiency and uniformity in the processing and use of certain health data. Substantial cost savings was the major driver for including the language in HIPAA. At the same time, Congress acknowledged that a streamlined electronic health information network posed heightened risks to patient privacy, as collecting and sharing health information moved out of a filing cabinet available to a few and into a linked online network available to many. Congress intended the privacy law timeline – which is a part of the administrative simplification section of HIPAA– to coincide

with the implementation of the uniform transaction and code sets, as well as the security rules. Both Congress and the Executive Branch recognized that a key to the success of a national health information infrastructure was to build privacy and security rules in at the outset. In fact, a report released in June 2003 by the Connecting for Health public/private collaborative of the Markle Foundation reached the same conclusion.

Myths and Facts

Both the 1996 Congress and the two recent administrations agree that a privacy law is needed to ensure that sensitive personal health information can be shared for core health activities, with safeguards in place to limit the inappropriate use and sharing of patient data. The HIPAA privacy rule takes critical steps in that direction to require that privacy and security be built in to the policies and practices of health care providers, plans, and others involved in health care. Despite the law's clear purpose and scope, a lack of widespread and consistent public education, training, and technical assistance over the past 2 and one half years, has given rise to a number of persistent and destructive myths.

The following are some common myths regarding the Rule and the facts about what the law actually says.

Myth #1: One doctor's office cannot send medical records of a patient to another doctor's office without that patient's consent.

FACT: No consent is necessary for one doctor's office to transfer a patient's medical records to another doctor's office for treatment purposes. The Privacy Regulation specifically states that a covered entity "is permitted to use or disclose protected health information" for "treatment, payment, or health care operations," without patient consent. As HHS explains, "treatment" includes "consultation between health care providers regarding a patient and referral of a patient by one provider to another." HHS states that providing health records to another health care provider for treatment purposes "can be done by fax or other means." §§164.502(a)(1)(ii), 164.506(a), http://www.hhs.gov/ocr/privacysummary.pdf (page 5), http://www.hhs.gov/ocr/hipaa/ (FAQ section, page 1, questions 6 & 12).

Myth #2: The HIPAA Privacy Regulation prohibits or discourages doctor/patient emails.

FACT: The Privacy Regulation allows providers to use alternative means of communication, such as email, with appropriate safeguards. Doctors and other healthcare providers may continue to communicate with patients via email. Both the HIPAA Privacy and Security Regulations require providers to use reasonable and appropriate safeguards to "ensure the confidentiality, integrity, and availability" of any health information transmitted electronically, and to "protect against any reasonably anticipated threats" to the security of such information. Therefore, a covered entity is free to continue using email to communicate with patients, but should be sure that adequate safeguards, such as encryption, are used. §§ 164.522(b)(1)(i), 164.306(a)(1)-(2), (d)(3)(i)-(ii), 164.312(e)(2)(ii).

Myth #3: A patient cannot be listed in a hospital's directory without the patient's consent and the hospital is prohibited from sharing a patient's directory information with the public.

FACT: The Privacy Rule permits hospitals to continue the practice of providing directory information to the public unless the patient has specifically chosen to opt out. The Regulation states that a health care provider, such as a hospital, may maintain a directory that includes the patient's name, location in the facility, and condition in general terms, and disclose such information to people who ask for the patient by name. The patient must be informed in advance of the use and disclosure and have the opportunity to opt out of having his or her information included in the directory. Emergency situations are specifically provided for in the Regulation, so if the patient is comatose, or otherwise unable to opt out due to an emergency, the hospital is permitted to disclose directory information if the disclosure is consistent with the patient's past known expressed preference and the provider determines disclosure is in the individual's best interest. The provider must provide the patient with an opportunity to object, "when it becomes practicable to do so." Any more restricted uses of directory information, such as requiring patients to ask to be listed in, or opt into, the directory, are either the hospital's own policy or confusion about the Privacy Regulation.
§164.510(a), http://www.hhs.gov/ocr/privacysummary.pdf (page 6), http://www.hhs.gov/ocr/hipaa/ (FAQ section, page 2, question 37).

Myth #4: Members of the clergy can no longer find out whether members of their congregation or their religious affiliation are hospitalized unless they know the person by name.

FACT: The Regulation specifically provides that hospitals may continue the practice of disclosing directory information "to members of the clergy," unless the patient has objected to such disclosure. Any requirement that the patient must list a specific church or any limitation on the practice of directly notifying clergy of admitted patients is either an internal hospital policy or based on a confused reading of the law.
§ 164.510(a)(ii)(A) http://www.hhs.gov/ocr/privacysummary.pdf (page 6).

Myth #5: A hospital is prohibited from sharing information with the patient's family without the patient's express consent.

FACT: Under the Privacy Rule, a health care provider may "disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual," the medical information directly relevant to such person's involvement with the patient's care or payment related to the patient's care. Uses and disclosures "for involvement in the individual's care and notification purposes" are clearly permitted. The Rule states that if the patient is present, the health care provider may disclose medical information to such people if the patient does not object. If the patient is unable to agree or object to disclosure because of incapacity or an emergency circumstance, the covered entity may determine whether the disclosure is in the best interests of the patient. The professional judgment of the health care provider should inform any decision regarding disclosure of protected health information to a family member or friend who is involved in the patient's care, as these disclosures are permitted, but not mandatory. If a hospital or other health care provider refuses to provide any relevant medical information to family members, it is again, the hospital policy, and not required by the Regulation.
§ 164.510(b)

Myth #6: A patient's family member can no longer pick up prescriptions for the patient.

FACT: Under the Regulation, a family member or other individual may act on the patient's behalf "to pick up filled prescriptions, medical

supplies, X-rays, or other similar forms of protected health information." The Regulation permits the health care provider to reasonably infer that doing so is in the patient's best interest and in accordance with professional judgment and common practice. HHS specifically explains that the Rule "allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient." Similarly, HHS issued guidance and a press release on July 6, 2001 that explicitly stated that "the rule allows a friend or relative to pick up a patient's prescription at the pharmacy." Therefore if pharmacies prohibit this common practice, it is their own policy, not one mandated by the HIPAA Privacy Regulation.
§ 164.510(b)(3), http://www.hhs.gov/ocr/privacysummary.pdf (page 6).

Myth #7: The Privacy Regulation mandates all sorts of new disclosures of patient information.

FACT: As HHS states, disclosure is mandated in only two situations: to the individual patient upon request, or to the Secretary of the Department of Health and Human Services for use in oversight investigations. Disclosure is permitted, not mandated, for other uses under certain limits and standards, such as to carry out treatment, payment, or health care operations, or under other applicable laws. Disclosure of protected health information has always been permitted for purposes such as national security, public health monitoring, and law enforcement, as well as many others. The Privacy Rule requires that patients be informed, through the notice of privacy practices, of these uses and disclosures. Nearly all of these uses and disclosures are permissive, so health care plans and providers may choose not to use or disclose medical information. §§ 164.502, 164.508, 164.512, 164.520, http://www.hhs.gov/ocr/privacysummary.pdf (pages 4-11).

Myth #8: The HIPAA Privacy Regulation imposes so many administrative requirements on covered entities that the costs of implementation are prohibitive.

FACT: The White House issued a report in March 2002 estimating the costs of implementing privacy over ten years at approximately $17 billion and estimating the savings incurred from putting the transaction standards in place over ten years at approximately $29 billion, thus saving the health care industry $12 billion overall. Further, there will be additional savings in the long term because patients will have more faith in the

health care system, so they will be less likely to withhold vital information from their doctors, and will more readily seek care.

Myth # 9: Patients will sue health care providers for not complying with the HIPAA Privacy Regulation.

FACT: The HIPAA Privacy Regulation does not give people the right to sue. Even if a person is the victim of an egregious violation of the HIPAA Privacy Regulation, the law does not give people the right to sue. Instead, the person must file a written complaint with the Secretary of Health and Human Services via the Office for Civil Rights. It is then within the Secretary's discretion to investigate the complaint. HHS may impose civil penalties ranging from $100 to $25,000, and criminal sanctions ranging from $50,000 to $250,000, with corresponding prison terms, may be enforced by the Department of Justice. However, according to the interim final rule addressing penalties, HHS "intends to seek and promote voluntary compliance" and "will seek to resolve matters by informal means whenever possible." Therefore enforcement "will be primarily complaint driven," and civil penalties will only be imposed if the violation was willful. Such penalties will not be imposed if the failure to comply was due to reasonable cause and is corrected within 30 days from when the covered entity knew or should have known of the failure to comply. The standard is even higher for imposing criminal penalties. §§ 160.306, 160.312 (a)(1), 160.304(b), 42 U.S.C § 1320 et seq., http://www.hhs.gov./news/facts/privacy.html.

Myth #10: Patients' medical records can no longer be used for marketing.

FACT: Use or disclosure of medical information is explicitly permitted for certain health related marketing under the HIPAA Privacy Regulation. For example, communication about a plan's health related products or alternative treatments and services is not considered marketing for the purposes of the Rule—even if the health care provider is paid to encourage the patient to use the product or service. The 2000 version of the Privacy Rule required that patients be notified if the health care provider was paid to communicate about a health related product, be given the opportunity to opt out of future communications, and be informed of the identity of the source of the communication. The Bush Administration eliminated these safeguards from the Regulation. §§164.508(a)(3), 164.50, http://www.hhs.gov/news/press/2002pres/20020809.html.

Myth #11: If a patient refuses to sign an acknowledgment stating that she received the health care provider's notice of privacy practices, the health care provider can, or must, refuse to provide services.

FACT: The HIPAA Privacy Rule grants the patient a 'right to notice' of privacy practices for protected health information, and requires that providers make a "good faith effort" to get patients to acknowledge they have received the notice. The law does not grant health care providers the right to refuse to treat people who do not sign the acknowledgement, nor does it subject the provider to liability if a good faith effort was made. A health care provider or health plan "must provide a notice that is written in plain language" that informs the patient of "the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information." The HIPAA Privacy Rule requires a covered health care provider with direct treatment relationships with individuals to give the notice to every individual no later than the date of first service delivery to the individual, to provide a copy of the notice to the patient upon request, to post a copy of the notice in a prominent location, and to "make a good faith effort to obtain a written acknowledgment of receipt of the notice" except in emergency situations. The acknowledgment of the receipt of notice of the privacy practices is not a consent for treatment. It is not an authorization for the release of medical records. A patient's signature acknowledging receipt of the notice, or her refusal, does not create or eliminate any rights, so it should not be the basis for providing or refusing treatment.
§ 164.520(b)(1), (a)(1), (c)(2)(i)-(iii)

Myth #12: The HIPAA Privacy Rule imposes many new restrictions on hospitals' fundraising efforts so that fundraising becomes almost impossible.

Fact: According to the Rule, a hospital may use, or disclose to its "business associate" or an institutionally related foundation, demographic information and the dates of health care provided to an individual "for the purpose of raising funds for its own benefit, without an authorization [from the patient]." Such use or disclosure is not permitted unless disclosed in the notice of privacy practices. Any fundraising materials that the covered entity sends to an individual must include a description of how the individual may opt out of future fundraising communications. Therefore, the Rule does not hinder fundraising in the first instance, and if a covered entity wants to target specific patients it must include

this information in its notice of privacy practices. Hospitals must also make reasonable efforts to ensure that those who decide to opt out of receiving future fundraising communications do not continue to receive such communications. §§ 164.514(f)(1)-(2), 164.520(b)(1)(iii)(B).

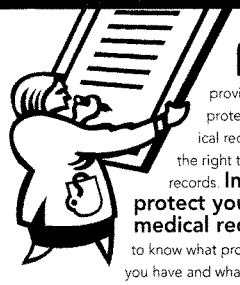
Myth #13: The press can no longer access vital public information from hospitals about accident or crime victims.

Fact: HIPAA allows hospitals to continue to make public (including to the press) certain patient directory information - including the patient's location in the facility and condition in general terms - unless the patient has specifically opted out of having such information publicly available. Thus, if a patient has not opted out of being listed in a hospital directory, and a reporter knows the name of an accident or crime victim, the reporter can request directory information from a hospital, including the condition of the patient. HIPAA does prohibit the hospital from releasing anything more than directory information, without the patient's authorization. This HIPAA provision, however, is not a change from most existing state laws, which protect the confidentiality of patient information to varying degrees. Further, the HIPAA Privacy Rule does not directly cover the media, so once a reporter obtains patient information, from any source, he or she is not restricted by HIPAA in how the information is used or disclosed.

Conclusion

We urge policymakers to look at the substantial progress being made by doctors, hospitals, and health plans in implementing the medical privacy rule. Policymakers, as well as covered entities, should recognize that the HIPAA privacy rule will improve the quality of care and access to care by fostering patient trust and confidence in the health care system. People will be encouraged to more fully participate in their own care, and public health and research initiatives will benefit from more reliable patient data. Also, we urge HHS and the professional and trade associations to continue to focus resources on pursing an aggressive public education campaign that separates the Myths from the Facts. Once fully and fairly implemented, the HIPAA privacy regulation will improve the quality of health care and broaden access to health care services by bolstering patient trust and confidence in the health system.

HEALTH PRIVACY: Know Your Rights



As of April 14, 2003, federal law provides some privacy protections for your medical records and gives you the right to see your own records. **In order to protect your personal medical records,** you need to know what protections and rights you have and what you can do if you believe they have been violated. The information in this brochure is an overview of those rights and protections. See the back of this brochure for resources that offer additional, more detailed information.

The rights and protections described inside apply throughout the United States. However, some states have their own laws that offer health care consumers stronger privacy protections and rights.

--> **Overviews of state laws available at www.healthprivacy.org.**

Your Rights and Protections

Notice

When you seek treatment from a health care provider or apply to a health plan for benefits, the provider or plan must give you a "Notice of Information Practices" that states your privacy rights and explains how they intend to use and disclose your health information. They are required to make a "good faith effort" to get you to acknowledge that you have received this notice by obtaining your signature. However, your signature is not required.

Access

You have the right to see, copy, and supplement your own medical records.

Copies of your records must be supplied to you within 30 days of your request. The holder of the records is allowed to charge you a reasonable fee for copying your records.

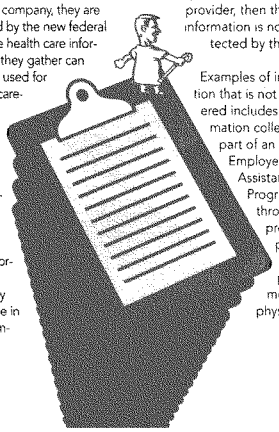
Security

Health care providers, plans, and "information clearinghouses" that collect, share and store your health information must have appropriate technical and administrative safeguards in place to protect your information.

Limits on Employers

Health care providers and health plans are barred from disclosing your identifiable health information to your employer.

In various circumstances, some employers also gather health-related information on their own. In those cases when the employer is acting in the capacity of a health plan or care provider, as in the case of a self-insured company, they are covered by the new federal law. The health care information they gather can only be used for health-care-related functions and they are prohibited from sharing that information with any one else in the company.



However, if an employer gathers personal health information, but is not acting as a health plan or health care provider, then the information is not protected by the law.

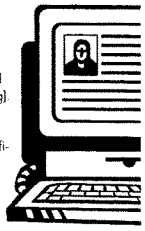
Examples of information that is not covered includes information collected as part of an Employee Assistance Program or through a pre- or post-employment physicals.

Psychotherapy Notes
Mental health providers can refuse to disclose psychotherapy notes to health plans without first obtaining a patient's voluntary authorization. Health plans may not condition the delivery of benefits or enrollment on obtaining an authorization from an individual.

Hospital Directories
You have the right to opt-out of having your name and health status publicly available in a hospital's directory. You may also limit the hospital from sharing medical information with family members.

Law Enforcement
In most cases, law enforcement officials must present some form of legal process—warrant, subpoena, summons—before a health care provider or health plan can disclose your health information to them.

When Your Rights Protections are Violated



If you believe that your health privacy rights or protections have been violated, there are several actions you can take:

Contact a privacy officer
Every health care provider and health plan covered by the federal health privacy law must appoint someone on their staff as a privacy officer. If you experience a problem related to the privacy of your medical records or access to them, you might want to contact this individual in an effort to resolve the problem.

File a federal complaint
You may also choose to file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights, the federal agency charged with enforcing the federal health privacy law. This office has the authority to impose civil and criminal penalties if they find a violation of the law. Your complaint must be filed within 180 days of the incident.

The complaint process is outlined at www.healthprivacy.org. A standard complaint form is also available on the website. You can also go directly to *www.hhs.gov/ocr/hipaa/*. Please be sure to send copies of your complaint to the Health Privacy Project, so that complaints and follow-up can be monitored.

Seek state-level recourse
There are officials in your state who may be willing to help you address violations of the federal privacy law and additional state privacy laws. Among those likely to help are your state attorney general [www.naag.org], your state insurance commissioner [www.naic.org], and a state medical board [www.fsmb.org]. See the websites to find your state's officials.

Lawsuits
You do NOT have the right to sue a health care provider or health plan for a violation of the federal privacy law, but a documented violation of the federal law may strengthen a privacy case you bring in state court.

Information Resources

Health Privacy Project
www.healthprivacy.org

HHS Office for Civil Rights
www.hhs.gov/ocr/hipaa/

Founded in 1997, the Health Privacy Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level. Originally a part of the Institute for Health Care Research and Policy at Georgetown University, the Project is currently an independent, nonprofit 501(c)(3) organization.

HEALTH PRIVACY PROJECT

1120 19th St NW, 8th Floor
Washington DC 20036
phone (202) 721-5614
fax (202) 530-0128
www.healthprivacy.org
info@healthprivacy.org

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

I don't think there's anyone on this committee, certainly not the Chairman, who doubts the value of and the importance of why Congress moved in the direction it did, not only for the very reasons you talked about—individuals denying themselves care for fear of a disclosure—but also the reality of the march of medical science. We all understand a doctor and medical professional's relationship to a patient and what that professional may know simply by medical science's ability today to determine certain kinds of things we didn't know that might determine future decisionmaking for the part of the patient that we as a society ought not be disclosed beyond that is critically important. I hope that we work our way through it.

My intent is not to cast a shadow over the importance of the privacy, but to make sure that we do it right, that we streamline it as best we can, that we get the informational flow out so that it doesn't become an impediment. It was not intended to be. So I thank you for that testimony.

I'm going to have to leave, but I must tell you, I am pleased to be joined by my colleague, Senator Peter Fitzgerald, who is going to carry on with the questioning. The first question he's going to ask, I do believe—I'm going to set him up for it—is a question that you, Cathy, alluded to, and some of you did, and I would like for the record for you to assess the announcement that you heard this morning from CMS as it relates to style of implementation, method, process to the legacy clause and all of that, and what that's going to mean in the short term as we work our way through this very complicated bureaucracy or regulatory process that we have set ourselves into with HIPAA.

Last, let me thank you all for being here, and especially let me thank the Senator for joining us this morning as a member of this committee to ask some very important questions for the record. Thank you.

Senator Fitzgerald. [Presiding.] Senator Craig, thank you very much.

I did want to ask you your thoughts on CMS' announcement this morning. Do you believe their willingness to extend the time past October 16 for filing claims under the old system will have a positive effect, and do you think any additional steps are needed? Anybody on the panel, I would encourage you to respond.

Ms. TREADWAY. Mr. Chairman, I would say that it is much appreciated that CMS has recognized that we will not be ready October 16, and taking the opportunity to extend that so that the health plans can accept both legacy claims and the HIPAA compliant claims.

However, as I mentioned in my statement, as we look at Idaho, not all systems can take both HIPAA compliant claims and legacy. It's one or the other. The State of Idaho Medicaid is in that exact situation. So even though it will help, it still has a long ways to go before we will not be experiencing delays of payment.

In addition, I also mentioned that we need guidance on whether they can accept and process and pay HIPAA compliant claims that don't have all the data elements that are required. All the new elements that are required are not necessarily needed to process pay-

ment. We do not want to see health plans being able to deny claims that they could process and pay. In Idaho, we do not have prompt payment legislation. That means there is no incentive for health plans to make that extra effort to get those claims paid. We are very fearful there will be significant delays in payment, which are going to affect our clinic's ability to provide care for our patients.

Senator FITZGERALD. Miss Fox.

Ms. FOX. Yes, I would like to comment. Thank you. I would like to comment both with respect to Medicare and as a private payer. Many of our plans contract with CMS and are actually the day-to-day processors of the Medicare claims. So we believe that their announcement today is very good news.

Both our Medicare contractors and private payers are very concerned that the low level of provider readiness could, if you don't have an announcement like this, result in providers returning to paper claims. Paper claims are expensive, both on the part of the provider and the payer, and could involve significant delays in payment because you would have to hire so many more people to process those paper claims. Under CMS' announcement, Medicare has announced that they will process the old electronic formats so that providers won't have to revert to paper if they're not ready for October 16.

On our private side, we are now polling our plans. Our plans are prepared. They do have contingency plans that would also allow existing legacy claims to be submitted and processed after October 16, and we are now polling our plans to see to what extent they are going to deploy them consistent with CMS' guidance.

I would add, however, that one of the recommendations made by MGMA is just not doable. What they are asking is that CMS tell payers that they must process a partially complete HIPAA claim. The whole purpose of standardizing these HIPAA electronic claims is so that a provider, when they submit a claim to Aetna, Cigna, Blue Cross or Medicare, knew that once they filled out the claim, that was an acceptable claim for all payers.

If you start saying you're only going to fill out 60 percent for one payer, 70 percent for another payer, you basically return to what we're trying to get away from, which is a lot of variation by payers instead of standardization. So we are very committed to the standardization and we're very committed to smoothing transition to HIPAA and assuring cash-flow to providers. We believe by plans continuing to process existing legacy claims after October 16 for some period of time the objective of smoothing the transition will be met.

Senator FITZGERALD. Any other comments on that?

Ms. GREALY. Senator, I think, whether we're talking about the transaction code sets or we're talking about the Privacy Rule, the CMS approach really represents something that I think is very important, that the government, whether we're dealing with CMS or the Office of Civil Rights, act as a working partner and collaborate with the health care industry as they're trying to implement these very complex rules. So I think, symbolically, it's very important that they're taking that approach, they're listening to what health care providers and plans are saying, and trying to work through these issues with them.

Senator FITZGERALD. I would think you would all agree that to have uniform transaction rules will really be a good thing and will take some costs out of the health care system ultimately, after the initial transition phase.

Ms. FOX. I think we need to look at that carefully. I think there are a lot of benefits, but I think it's important to note that these HIPAA transaction code sets is phase one. There are lots of phases on the horizon, so it's not like you do this and you're done. Really what's envisioned is constant change for the next several years. So I think we——

Senator FITZGERALD. How many phases does HIPAA bring us through?

Ms. FOX. We don't know the answer to that question, actually. There is lots of different phases on the horizon. There are three standards that are due out within the next year, and CMS is already looking at modifications to the ones we're just now struggling to implement. So we are recommending that we get a stakeholder commission to really look at that, how many phases are we talking about, where are we headed, how are we getting there, are we getting there in the most cost-effective and efficient manner, and make sure that everybody has a consensus on how we're proceeding.

Senator FITZGERALD. Along those same lines, I wonder if each of you could summarize briefly the best dollar estimates that you are aware of regarding the costs incurred by the entities you represent in complying with the new HIPAA transaction rules, and with the privacy regulations.

Ms. GREALY. Well, we represent the entire health care industry, and we're focusing just on the Privacy Rule. That's what we have worked on.

As I said in my statement, HHS put out an estimate of $17.5 billion over 10 years. Blue Cross Blue Shield had an estimate of, I believe it was $45 billion——

Ms. FOX. Forty-two.

Ms. GREALY [continuing.] Of $42 billion. As you can see, it's a rather disparate range.

I don't think we'll really know. We know that it is in the tens of billions of dollars, and that $17.5 billion is quite a low estimate. Yes, it's an important issue, but I think we need to look at how else could those resources be used. How else could the funds for those personnel that are being hired, been used. What other hires could have been done—more nurses at bedside probably would be a preference. So we hope we can strike a balance.

As Senator Craig said, let's see if we can streamline this process, make it as cost efficient as possible, while we're trying to meet the real concerns of the patients.

Senator FITZGERALD. Do you think the costs are appropriate to the benefits that are likely to be achieved?

Ms. GREALY. Do I think we could have done it in a less prescriptive, less regulatory way? Yes, I think we could have done it more efficiently and cheaper.

Senator FITZGERALD. Achieve the same benefits?

Ms. GREALY. Achieve the same benefits.

Senator FITZGERALD. Is that HHS' fault or is that Congress' fault because Congress mandated HHS to promulgate regulations if we didn't act.

Ms. GREALY. I think the regulations could have been much more streamlined. We have made progress and we have made improvements, and we will have the opportunity to do that from year to year. But the initial regulation that we were dealing with was voluminous and way too detailed and way too prescriptive. So I think we have made improvements in it and hope to continue to do that.

Ms. GOLDMAN. I think it's really important when we're talking about cost to factor in both what the White House has estimated the cost to be which some of the testimony presented here does not acknowledge. The White House estimated that the cost associated with putting the Privacy Rule in place would be offset many billions of dollars by putting the transaction and code set regulations in place.

In fact, when Congress put the mandate in HIPAA back in 1996, many of us were involved in that process, and the reason the privacy regulation went into HIPAA is because the industry was pushing very hard to create that uniformity in the transaction and code sets, to create a common language for how health information would be coded and shared.

There was an acknowledgement that putting privacy in place at the same time was a prudent measure, that we would be increasing risk obviously to privacy and discrimination by creating a national health information infrastructure, but that that was critical to moving forward with health care. So we could build privacy and security in at the outset, there was an acknowledgement by Congress and by most of us sitting here in this room that we had to do that together and that it would save money to do it together and it was the right thing to do.

The White House estimates I think have been quite clear, that there will be a substantial cost savings ultimately, and we need to think about that.

As I said earlier, it's very important to also factor in saving money from improving quality of care and broadening access to care and having more reliable data for research. Most of the estimates don't include that because I think it's a tough thing to measure.

Ms. TREADWAY. Mr. Chairman, I would just like to bring this back down to the provider level. This is an unfunded mandate. These costs are creating additional costs for us to provide care for our patients, and skyrocketing the costs for health care. If you compound that by malpractice insurance and all of the other government regulations that we're facing, it is a struggle for physicians.

As I talk to the different small groups in our State, they are very worried about their ability to keep up with the government regulations. As we've mentioned, it's volumes and volumes of information, trying to read it, trying to understand it. They don't have the staff to do that. They are there to take care of patients.

There may be additional savings down the road, but at this point in time we are worried about how to keep our doors open and to take care of patients in light of not knowing if we're going to be paid for our service and trying our best to work within the system

to comply with all of the government regulations that are there. We are very concerned, and the costs are nationwide, when you come down to an individual provider, the dollars are not there to comply and it's unfunded. So we are being forced to attempt to comply and it just skyrockets our costs of providing health care.

Ms. GREALY. Mr. Chairman, we also were looking for national uniformity with the Federal Privacy Rule. We did not get that. The Healthcare Leadership Council has had to fund a one million dollar study so that we could provide information to all of our members, members of the confidentiality coalition, as to what is the interplay between the Federal law and regulations and the various State regulations. So this Federal regulation is merely a floor. It's not a ceiling. That is something that every provider is going to have to be aware of.

I think perhaps you are seeing a bit of hyper-compliance. I think that has a lot to do with hospitals that have been involved in various investigations for what were billing errors, and yet having that characterized as fraud. I think everyone has taken compliance extremely seriously, and perhaps to the extreme, but feel that they've got to make this investment to make sure they're doing it the right way so that they are not subject to an investigation or a civil or criminal complaint.

Senator FITZGERALD. Why do you believe so many parts of the health care system are having such continuing difficulty complying with the new transaction rules? What is it about the new rules that makes them so difficult to comply with?

Ms. FOX. We think there's three reasons why it's so difficult. One is there is just a general lack of awareness about the regulation itself. Second, there is a lack of understanding about the cost and the scope of the regulation.

I think a mistake that all of us made, quite frankly, Mr. Chairman, is that we had representatives working to develop these standards at the front end, but the people we had sitting around the table were our information technology staff, who while they are quite capable, they look at things from a systems only standpoint. What we realized in looking backwards is that when you change a code and you change these formats, and you now say, "I'm only going to have this data or that data, it has a ripple effect on the entire operation—whether you're a payer, whether you're a hospital or a clinic—that we, quite frankly, just didn't understand." When you change that code, it can change your provider payment, it can change how you detect fraud and abuse, it could change your quality improvement programs.

The way that our systems work is we piggyback everything on a single code. So once you change that—and the information technology staff just really didn't identify those issues. So I think we just didn't realize how expensive and big this regulation was to begin with.

Senator FITZGERALD. What does that mean in concrete terms? How can we improve things for you? If you had two or three changes that you could make to the regulations, what would they be?

Ms. FOX. It's not the regulation itself. It's really the process we would like to see changed. At the front end we would like to see—

all of the stakeholders, involving our whole operation, not just our information systems people. Second, we think it's critical that we get a true cost-benefit analysis done collectively. Let's really look hard at what those costs and benefits are so we all agree on that.

Third, it's critical to pilot test it. I think it's a big mistake that we didn't pilot test this. When you pilot test it, then you identify what the issues could be, what are the possible unintended consequences. Once you pilot test it, you can make sure that, before you tell the whole country to do something, you have identified the wrinkles.

Senator FITZGERALD. Well, it's not being pilot tested.

Ms. FOX. I'm sorry?

Senator FITZGERALD. It's not being pilot tested, right? The whole country is doing it.

Ms. FOX. I'm saying going forward, and when we do the next stages of these regulations, we need to learn from the mistakes we made this time. I think now what we need to do is—I think we're getting there. I think we need to employ contingency plans, make sure that providers get over this hump, but I think we really need to learn lessons from this experiment.

Ms. TREADWAY. Mr. Chairman, I would like to comment on that, also.

Part of the issue that we dealt with is that we didn't get final information from CMS until February of this year. Many of the vendors were waiting for that direction before they finalized their programs.

This is an extremely complex process. We are dependent on the health plans, the clearinghouses and our software vendors, to all have their ducks in a row before we can begin testing. So as we work on it, we have been attempting to test for over a year now, and finally became a beta test site to begin testing, and felt that we were starting to move forward. It took two solid months before we got anything that ever went through. It just said beta file error. You have to be able to test real data.

Then we found out they're not even testing with Idaho payers. It's very, very complicated. If there had been staggered implementation dates so that health plans and clearinghouses and vendors had different staggered dates for implementation, it would have made it easier from the providers' standpoint to go with.

The other thing we're dealing with is they do not have to give us the missing data elements when we have a claim that's denied. All of this is just very, very complicated. I think the complexity is really a struggle for all of our small providers because we don't have experts helping us through this.

Senator FITZGERALD. I have a question for Miss Fox. In your testimony you point out that HIPAA's efforts to achieve electronic claims standardization are going on, even as other uncoordinated efforts are being launched elsewhere in the government to promote greater use of electronic systems in health care, such as electronic medical records.

How can we in government better go about advancing the goal of bringing new e-technology to health care without breeding even more confusion?

Ms. FOX. We are recommending that Congress set up a stakeholder commission that would really look at where is the vision, where do we all want to go. A lot of people have a vision that we want to have electronic medical records that can move from doctor to doctor across the country. To get there, you really need to take these new standards we're doing today as a continuum to get there.

If that is the vision, what is the smartest way of getting there? Is that the vision everybody agrees to? What should come next? What codes should we change? People are talking about going from ICD–9 to ICD–10. That's the coding system for diagnosis that hospitals and other providers use. People are talking about that as the next step. We have a consultant that's looking at it and saying that might not be the next step. You might want to actually describe the services, for example, like how you set an arm, and maybe you don't even—He was raising yesterday with us that maybe you don't even need going to a replacement for ICD–9 if you describe your services in a standard way.

These are the kinds of issues that I think we all need to discuss around the table, and walk through what are the steps to get you to the end result, how much money is it going to cost, what's the most efficient way to get there, what's the priority, and then let's go forward in a smart way so that we're not wasting resources.

Senator FITZGERALD. So you would like to see Congress set up a commission that could hash this out.

Ms. FOX. Yes.

Senator FITZGERALD. Has anybody introduced a resolution in either the House or the Senate?

Ms. FOX. No. We are talking to people now about such a proposal.

Senator FITZGERALD. OK. So you might be working on that.

Ms. FOX. Yes.

Senator FITZGERALD. I guess I would ask all of you this, but especially Miss Goldman and Miss Grealy. In your estimation, what are the most troublesome areas in the new privacy regulations when it comes to patient or provider confusion?

Ms. GOLDMAN. I think that what we saw initially we are now seeing die down. As Director Campanelli testified earlier this morning, he's only getting about a third of the questions now a few months into the implementation phase.

But I think the things that continue to trouble me are, one, the misunderstanding that doctors can't share information to treat patients. You see reports in the newspaper all the time, and I talk to doctors who say, if I refer a patient to another doctor, they won't then talk to me about the patient or information can't be shared back to me to treat the patient. That's just wrong. It's not even a question of interpretation. It's just wrong. I think it needs to be absolutely clear from the professional and trade associations, from OCR, from the State regulators, that doctors and other health care providers can share information to treat patients without having to get consent.

Picking up prescriptions, visiting relatives in the hospital, again the status quo in some ways, the presumption that most of us share, that information should flow freely to treat people, to pay for their care, and to allow us, as family and friends, to be able to take

care of those we love. So those are the things that I think we absolutely have to address.

Of course, somewhere down the road, once there is a clear understanding and we do clarify the myths and facts about the privacy regulation, we would like Congress to take up what we consider to be some of the regulation's weaknesses, some of the gaps in the law, some of the areas where the law doesn't go far enough. I realize this may not be the best time to bring that up, but it is part of our long-term agenda, to make sure the law is more enforceable, to make sure it does cover employers directly when they do collect information themselves.

Senator FITZGERALD. When was your group formed, Miss Goldman?

Ms. GOLDMAN. When?

Senator FITZGERALD. Yes.

Ms. GOLDMAN. The Health Privacy Project was created at the end of 1997.

Senator FITZGERALD. Where does it get its funding?

Ms. GOLDMAN. We get funding from foundations primarily.

Senator FITZGERALD. OK.

Ms. GOLDMAN. Anybody who would like to contribute to the Health Privacy Project can see me after the hearing. [Laughter.]

Senator FITZGERALD. Miss Grealy, would you have a response about what areas are the most troublesome in the privacy regulations?

Ms. GREALY. Mr. Chairman, I participated in a town hall meeting in Baltimore on behalf of Congressman Cardin recently. As Miss Goldman has pointed out, there is a lot of confusion as to what information can be shared between health care providers. We heard quite a bit from social workers, who had the responsibility of monitoring mentally disabled adults in group homes and whether they could get information from physicians to make sure those adults are being treated appropriately.

As I said earlier, I think there is a real sense of hypercompliance. Everyone was told you could only share the minimum amount of information necessary, or that you have to have the patient's prior written consent before you can do certain things. There is a lot of confusion. We have to do a lot of education.

I think the Office of Civil Rights is doing a good job, but I'm not sure the general public and every provider thinks of going to the HHS website. So we are doing our best to try to get that information out there. As I said, we participate in town hall meetings in congressional districts; we do Hill staff briefings, again trying to tell people what this rule actually does.

There are areas where we can reduce the regulatory burden. One in particular that I cite in my testimony is maintaining records of when you make disclosures. With the hundreds of millions of patients that are admitted to hospitals, that are treated by physicians, trying to track all of that is just overly burdensome and something we think can be streamlined.

So we look forward to working with HHS and trying to refine this rule as we go forward. We think we can make it more simple. But we do have to do a lot more educating of the public and educating the providers. It isn't that clear. I think we who have been

immersed in the rule understand it pretty well, but I think these questions still normally arise and we do have to do better on education.

Senator FITZGERALD. Miss Treadway, I'm wondering if you could estimate for the panel what proportion of your time has been spent in the last couple of years working on or getting ready for HIPAA compliance.

Ms. TREADWAY. I would estimate that of my time in my clinic, it has been in excess of 10 percent, 10 to 12 percent of my time that is spent on HIPAA privacy and on working within our group and within the State, trying to educate the providers and the administrators throughout the State on the regulations and what they need to do to prepare for that. I would say probably 10 to 12 percent of my time alone has been spent over the last couple of years doing that.

Senator FITZGERALD. Do you feel your colleagues elsewhere in Idaho who are providers have become, as we've gotten closer to the implementation, better familiarized with the regulations?

Ms. TREADWAY. I would say yes. Our Idaho HIPAA Compliance Coordinating Council has done a road show throughout Idaho on three separate occasions. The most recent one was this Friday. We had 121 participants in the morning and 121 in the afternoon, and a waiting list of people to get in on the HIPAA education. We had representatives from Medicare, Idaho Medicaid, Blue Cross of Idaho, Blue Shield of Idaho. They asked a question out there and asked in the morning session how many were ready for HIPAA codes and transactions, and three out of 120 raised their hand, that said they thought they were ready. Mostly that was because their vendors had assured them that they would be ready to submit and be able to process claims. A lot of them are hoping to begin testing. Some of them don't even have the software loaded on their computer systems yet.

So yes, are we fearful in Idaho, and yes, they are trying to get information across the State. When they have done these meetings, we've had huge attendance at them.

Senator FITZGERALD. I wonder what HHS or the major provider organizations could be doing better to alleviate the confusion that you describe. It sounds like there are a lot of seminars being conducted and people certainly have the opportunity to go to those seminars, although you said there was a waiting list and not everybody was able to get in to them. But it would seem to me there would be plenty of opportunities to familiarize yourself and your organization with the new regulations.

What else could HHS being doing?

Ms. TREADWAY. I think continual education, continually working on simplification, are two really important parts of it. I think the steps CMS took today to work toward allowing an extension of that deadline is helpful. Unfortunately, we are within 3 weeks of the implementation of this. As we found out from the privacy rules, when the original regulations come out, and then when they do the loosening or the changes in them, some people read the original and they don't get all the changes. So as we look at these constant changes, it is very, very difficult to say am I dealing with the cur-

rent regulations, or which area of the regulations am I truly dealing with.

If I went to a seminar 2 years ago on any of these regulations, and I felt I was up-to-date on them and I didn't go to the most current one, I would have missed the entire process because things have changed so drastically during that time.

As Senator Craig mentioned, there were 102,000 words in this legislation. You look at that and it's massive for a small doctor's office. In Idaho, the average is two-and-a-half physicians per clinic. You have five or six staff that are trying to implement these regulations. How can they even hope to be able to comply with it?

Senator FITZGERALD. We have just 6 minutes left before I have to go and make a vote, so I'm going to bring this meeting to an end. But I just want to ask one more question for Miss Grealy.

Your organization, the Healthcare Leadership Council, has taken the lead in launching an industry-wide study examining differences between the Federal Privacy Rule and each State's privacy rule. Why is this study necessary, and approximately how many States have more stringent requirements than HIPAA?

Ms. GREALY. Many States. I don't have the exact number.

The reason we undertook this study was because Congress did not make this privacy rule or law preemptive of State law.

Senator FITZGERALD. Except if it's a more lax privacy rule.

Ms. GREALY. So it establishes the regulation as a floor as opposed to a ceiling.

Senator FITZGERALD. Right.

Ms. GREALY. So we don't have that single national uniform standard.

Senator FITZGERALD. Would you like that?

Ms. GREALY. Yes, we would.

Senator FITZGERALD. Miss Goldman wouldn't, I guess.

Ms. GREALY. We had asked also that, given that we didn't get that, that HHS provide guidance and interpret what is the difference between the Federal regulation and the State law. HHS has refused to do that. So that's why it fell to the industry——

Senator FITZGERALD. Well, they're not in the business of interpreting the States' laws.

How many States have tougher privacy laws?

Ms. GREALY. I'm sure Miss Goldman would know. I believe it's the majority.

Ms. GOLDMAN. We did a similar analysis in 1999. It's not as targeted to the industry as the Healthcare Leadership Council's analysis, which is being sold to some in the health care industry. Ours is, as I said, available for free.

What we found was that most of the privacy regulation as it currently reads will preempt most State law, because most State law is less comprehensive and less specific.

Senator FITZGERALD. How many States have tougher laws?

Ms. GOLDMAN. Well, where the States do have tougher laws, there are a couple of States where, even in some of the kind of broad areas, like access to records or limitation on disclosure that you might find in California, for instance, there are more stringent State laws in those broad areas.

Senator FITZGERALD. Any State besides California?

Ms. GOLDMAN. California comes to my mind. Minnesota does as well.

But most States have these condition-specific laws that the privacy regulation——

Senator FITZGERALD. Now, I have to ask you this. Do you think it's a good thing for companies to have to comply with different laws in all the different States? I mean, don't you think that adds a lot of cost to the health care system and cuts down on the affordability and availability of health care?

Ms. GOLDMAN. Well, I'm glad you asked that, because prior to the privacy regulation taking effect, every health care organization in the country had to comply with 50 different State laws, patchwork laws.

Senator FITZGERALD. That's true.

Ms. GOLDMAN. The privacy regulation, in many ways, created substantial uniformity. In most of the Federal laws in this country, we don't preempt State law. We might preempt State law that's weaker——

Senator FITZGERALD. Isn't she right, Miss Grealy?

Ms. GREALY. We lobbied strongly for Federal legislation that would establish that uniform standard, to avoid exactly what you're saying, the additional cost. So now, going forward, you will always have to check what's happening with the State law as it's updated, as it's changed. So is that really a cost we need to incur in the system?

Senator FITZGERALD. I'm sorry, Miss Goldman, but we're running out of time here. Is your organization lobbying in certain States to make the privacy laws tougher than the Federal laws?

Ms. GOLDMAN. Well, let me first say that we don't lobby, but we——

Senator FITZGERALD. Advocate?

Ms. GOLDMAN. Well, we have not actually advocated that. What we're trying to do is work with a lot of the same issues that some of the industry people are. We are working with a lot of the safety net providers, the community clinics——

Senator FITZGERALD. Are you supporting tougher——

Ms. GOLDMAN. Not necessarily.

Senator FITZGERALD. So you're not supporting tougher privacy laws in any of the States?

Ms. GOLDMAN. We haven't gotten into that area at all. We're just trying to help folks sort out where the privacy laws in the States and the Federal laws come together.

Senator FITZGERALD. OK. Miss Fox, you wanted to say something, and then I am going to have to adjourn the meeting. You have all been terrific witnesses and we appreciate it.

Ms. FOX. Thank you so much for letting me just add my two cents.

I think it's important to realize that we're not talking about here's the Federal privacy law and here's the State privacy law. The States have multitudes of privacy laws and they're buried in lots of little statutes. For example, there might be a privacy law that talks about AIDS patients, another privacy law that talks about maybe immunizations——

Senator FITZGERALD. But couldn't you argue that it's preempted by HIPAA?

Ms. FOX. You have to look at each individual provision in each statute. One State might have "x" number that aren't preempted, but lots of ones that are. So it's not simply saying in California it is and in Nebraska it isn't. There are lots of different rules and you have to go provision by provision in lots of different State laws that are buried in lots of different statutes. So it's very complicated.

I'll tell you our plans are working through privacy and are very committed to it, but of all the things that they find difficult, it is the conflict between State and Federal rules, and if you're a provider and you're in DC and you practice in Maryland and Virginia, what are your rules? It's very complicated. That's why we're supporting HLC on this position.

Senator FITZGERALD. There is one conclusion I think I can safely draw—that HIPAA is probably very good for my profession, which is the legal profession.

Ms. FOX. Full employment.

Senator FITZGERALD. Full employment for lawyers, health care lawyers.

All of you have been terrific witnesses. I wish we had more time. I want to thank you for making the trip here. We will leave the record open for any Senators for a period of 2 weeks.

Thank you all very much. This meeting is adjourned.

[Whereupon, at 11:43 a.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM SENATOR LINCOLN TO HHS

Question. I am aware that CMS has a contingency plan ready to put into effect that would allow Medicare and Medicaid fiscal intermediaries to run dual systems to accept electronic billing submissions in either the current format or the HIPAA-compliant format. However, CMS hasn't made a decision to implement this plan yet. It seems reasonable to allow this considering the consequences to health care providers. When will you make this decision?

Answer. CMS announced its decision to implement the contingency plan for Medicare on September 23, 2003. Each state will make its own decision regarding implementation of it contingency plan.

Question. I have heard from providers in Arkansas that much of the privacy law is left up to interpretation. For example, the legal counsels advising the physicians and the legal counsels advising the hospitals often differ in their interpretation of the regulations, and thus many providers have questions. What services has the government provided in answering questions providers might have?

Answer. The Office for Civil Rights (OCR) has conducted, and is continuing to conduct, and extensive public education effort to produce and disseminate a wide range of guidance about various aspects of the Privacy Rule that need clarification or are of concern to the public and to covered entities, including providers. We do this through a variety of ways, such as by making presentations to educate various groups, providing a toll-free call-in line for questions, and by publishing Frequently Asked Questions (FAQ) and other guidance and technical assistance materials on our website. The following provides additional detail on each of these activities:

Presentations. OCR senior Privacy experts, from Washington DC and throughout our regions, have made well over a hundred presentations during 2003 alone. These include four national, all-day HIPAA Privacy Rule conferences, attended by some 6000 participants, sponsored in conjunction with universities and key industry groups, held earlier this year. In addition, OCR has conducted or participated in numerous telephone audio conferences.

Toll-Free Call-In Line. In conjunction with the Centers for Medicare and Medicaid Services (CMS), OCR offers a free call-in line, 1–866–627–7728 for HIPAA questions. Since April 1, combined phone-line operators and OCR staff have received and responded to some 14,000 calls related to the Privacy Rule.

Website at http://www.hhs.gov/ocr/hipaa/. Our website plays a key role in our outreach activities, and has enabled us to post and broadly disseminate information that provides additional clarification in helpful areas, and to clear up misconceptions when they arise. In turn, providers can use these posted materials to educate each other. From January through July 2003, OCR's Privacy Rule homepage received 847,800 visits. Some of the helpful materials on our website include: a comprehensive *Summary of the HIPAA Privacy Rule,* which is linked to more detailed guidance on particular aspects of the Privacy Rule; a *Covered Entity Decision Tool,* which interactively assists entities in determining whether they are covered by HIPAA; sample *Business Associate Contract Provisions;* targeted guidance materials explaining the research and public health provisions of the Privacy Rule; and fact sheets for consumers.

In addition, a key feature of our website, accessed over 1.2 million times since January of this year, is our database with over 200 searchable FAQs. The database is simple to use, and provides clarifications on many different aspects of the Privacy Rule, including many areas that are of particular interest and relevance to the provider community. For instance, there are a number of questions that address permissible disclosures among health care providers for treatment. Our website is also organized to be as helpful as possible and includes a link focused on materials we believe are of particular interest to small providers and small businesses.

We continue to develop guidance and other materials to educate covered health care providers and other covered entities about the Privacy Rule so that the Rule's implementation is effective and efficient, and does not impede a patient's access to quality health care. This includes continuing to develop FAQs as we become aware of misconceptions of other issues about the Privacy Rule that need clarification. We also are in the process of developing additional targeted technical assistance materials, focusing on explaining the Privacy Rule to consumers as well as specific industry groups, including smaller health care providers and institutional health care providers.

Question. Health care providers in Arkansas, particularly rural hospitals, have told me that because their older information technology systems require so much updating to comply with HIPAA they may not be ready by October 16. They say even with the grant money available to them, it is still tough financially. What is scary to them is that hospitals won't receive Medicare and Medicaid payments if they are not in compliance by the deadline, or if the fiscal intermediary is not in compliance by that time. What steps has CMS taken to identify those hospitals and other providers who continue to struggle with this (despite the fact that we gave them an extra year to comply) so that they are not faced with a huge financial crisis? Rural hospitals in Arkansas depend heavily on revenue from Medicare to keep their doors open.

Answer. CMS has taken a number of steps to ensure the smooth flow of payments after October 16, 2003. Fiscal intermediaries are in compliance; and, CMS has deployed its Medicare contingency plan to maintain provider cash flow and minimize operational disruption while trading partners work with Medicare to achieve full compliance. Furthermore, we understand that all States are prepared to adopt contingencies to keep Medicaid payments flowing.

In Arkansas' case, CMS has been working closely with the State for the past three years to provide technical information and funding at 90 percent federal financial participation matching rate for its Medicaid claims processing system.

Arakansas has said that the State's system will be able to accept HIPAA-compliant formats as early as October 13. Their backup strategy for providers whose systems are not yet HIPAA-compliant is for them to download from the website software developed by the State to enable all providers to submit HIPAA-compliant claims, together with code crosswalks which walk providers from the old codes to the new ones. As a fallback, providers also can use Direct Data Entry (DDE) to submit claims to the State. Claims would be rejected only if a provider does not utilize these various contingencies. The State is very sensitive to the cash flow requirements of small and rural providers and has made every effort to ensure payments will continue.

Question. I have heard from providers that new HIPAA requirements are being added daily, making it impossible for them to keep up. One provider said that they've noted 100 new requirements in a two-month period, Is this true?

Answer. No. The requirements have not changed since the Final Rule adopting changes to the HIPAA Electronic Transactions and Code Set Standards was published on February 20, 2003, which actually reduced the number of requirements. It is possible that as they have begun to test, providers are discovering that adjustments to their systems are needed in order to become compliant.

American Psychiatric Association

1000 Wilson Boulevard
Suite 1825
Arlington, VA 22209
Telephone: 703.907.7800
Fax: 703.907.1083
E-mail: ntrenti@psych.org
Internet **www.psych.org**
Contact: Nancy Trenti, J.D.

Statement of

The American Psychiatric Association

to

The Senate Special Committee on Aging

on

"HIPAA Medical Privacy and Transaction Rules:
Overkill or Overdue?"

September 23, 2003

The American Psychiatric Association (APA), a national medical specialty society, founded in 1844, whose over 38,000 psychiatric physician members specialize in the diagnosis and treatment of mental illness including substance use disorders, appreciates the opportunity to provide a statement on the Health Insurance Portability and Accountability Act (HIPAA) Electronic Transaction and Privacy Regulations. We thank the Committee for allowing us to provide this statement.

The American Psychiatric Association (APA) is pleased the Bush Administration, under the leadership of the Center for Medicare and Medicaid Services' (CMS) Administrator Tom Scully, has published the attached Frequently Asked Questions (FAQs) on the CMS website. The Bush Administration efforts to address concerns with the DSM-IV and ICD-9 in the HIPAA Electronic Transaction Regulation are critically important to psychiatrists and the mental health community, all other clinicians, health plans, providers, and clearinghouses.

Attached is a letter to Congressman Nancy Johnson that outlined our HIPAA concerns. APA is eager to work with the Administration to communicate the FAQs to health plans, providers, clearinghouses, and vendors. Additionally, the APA appreciates CMS announcing that it will implement a contingency plan to accept noncompliant electronic transactions after the October 16, 2003 compliance deadline. The contingency plan will ensure continued processing of claims from thousands of providers who will not be able to submit a HIPAA compliant electronic claim, meeting the deadline and who otherwise would have had their Medicare claims rejected.

The APA is very concerned with the inadequacies of key provisions of the administration's privacy regulations. However, the regulations do recognize: the general rule of non-preemption of greater 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; and the requirement that the entire medical record not be used in cases where a portion of the record will suffice, i.e. the "minimum necessary" requirement. Physicians can cite this provision when dealing with unreasonable health plan requests for information. Attached is the APA's testimony before the House Energy and Commerce Committee Subcommittee on Health.

The APA strongly believes that protecting and strengthening the confidentiality of the doctor-patient relationship is critical for providing the highest quality medical care. Patient medical records should only be used or disclosed by a health care plan, provider, and clearinghouse with the informed, voluntary, and non-coerced consent of the patient. Exceptions should be made for the unintended consequences of the prior consent requirement, such as when a patient's information is needed to fill a prescription or schedule a referral so there will be no delay in treatment. The patient's consent can then be obtained orally, by fax or mailed at a later time that is more convenient. Marketing loopholes should be closed. Thus, the APA supports H.R. 1709, the "Stop Taking Our Health Privacy (STOHP) Act of 2003". For your reference, we are attaching the APA's

medical privacy testimony before the Senate Health, Education, Labor and Pension Committee, the APA's comments to HHS on the proposed changes to the privacy regulation, and the APA's press release on the modifications made to the privacy regulation.

To assist APA members in meeting the HIPAA compliance requirements, APA has developed a packet containing educational materials and sample documents. This information can be accessed electronically, as one of our member benefits, in the "Members Corner" of the APA website (www.psych.org). As part of our extended member service, APA created an electronic bulletin board where members can ask questions about HIPAA as well as view questions previously asked by their colleagues and read the corresponding answers prepared by consultants with HIPAA expertise. The electronic bulletin has been used thousands of times. Additionally, APA has a HIPAA training program for psychiatrists and their staff.

Again, we thank the Committee for the opportunity to deliver this statement on the HIPAA Electronic Transaction and Privacy Regulations. Please do not hesitate to call on the APA as a resource, should there be any way in which we might be able to assist you.

The Center for Medicare and Medicaid Frequently Asked Questions (FAQs)

Question Can mental health practitioners, agencies, institutions and others still use DSM-IV diagnostic criteria, even though DSM-IV has not been adopted as a HIPAA code set?

Answer Yes. Adoption of the diagnostic criteria, which are used to establish a diagnosis, is outside the scope of HIPAA. Congress enacted HIPAA for the purpose of standardizing the form and content of certain electronic transactions, and not for the purpose of standardizing the diagnostic criteria applied by clinicians. The basic purpose for adopting code sets under HIPAA is to standardize the "data elements" used in the electronic processing of certain administrative and financial health care transactions. While the patient's diagnosis is a data element used in such transactions, the criteria considered by the clinician in reaching a diagnosis are not. Practitioners are free to use the DSM-IV diagnostic criteria—or any other diagnostic guidelines—without any HIPAA-related concerns.

Question In current practice by the mental health field, many clinicians use the DSM-IV in diagnosing mental disorders. Can these clinicians continue current practice and use the DSM-IV diagnostic criteria?

Answer Yes. The Introduction to the DSM-IV indicates that the DSM-IV is "fully compatible" with the ICD-9-CM. The reason for this compatibility is that each diagnosis listed in the DSM-IV is "crosswalked" to the appropriate ICD-9-CM code. It is expected that clinicians may continue to base their diagnostic decisions on the DSM-IV criteria, and, if so, to crosswalk those decisions to the appropriate ICD-9-CM codes. In addition, it is still perfectly permissible for providers and others to use the DSM-IV codes, descriptors and diagnostic criteria for other purposes, including medical records, quality assessment, medical review, consultation and patient communications.

Question The ICD-9-CM includes a glossary with definitions for mental disorders found in Appendix B. Are clinicians required to use these glossary definitions when using the ICD-9-CM codes?

Answer No. HIPAA does not require clinicians to adhere to the glossary definitions in Appendix B. The ICD-9-CM itself does not require clinicians to adhere to the glossary definitions. With respect to these definitions, the Introduction to the ICD-9-CM states only that Appendix B has been "included as a reference to the user…to further define a diagnostic statement." This statement suggests that the glossary definitions are advisory only, and not mandatory. While HHS has adopted the ICD-9-CM as a HIPAA code set for diagnosis, it has not mandated the use of the glossary definitions.

Question Has Medicare announced its contingency plan?

Answer Yes. On September 23, 2003 CMS announced that it will implement a contingency plan for the Medicare program to accept noncompliant electronic transactions after the October 16, 2003 compliance deadline. This plan will ensure

continued processing of claims from thousands of providers who will not be able to meet the deadline and otherwise would have had their Medicare claims rejected. CMS made the decision to implement its contingency plan after reviewing statistics showing unacceptably low numbers of compliant claims being submitted.

The contingency plan permits CMS to continue to accept and process claims in the electronic formats now in use, giving providers additional time to complete the testing process. CMS will regularly reassess the readiness of its trading partners to determine how long the contingency plan will remain in effect.

July 17, 2003

Honorable Nancy Johnson
Chairman
Subcommittee on Health
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Johnson:

I am writing on behalf of the American Psychiatric Association (APA), the medical specialty society representing 36,000 psychiatric physicians nationwide, in response to your kind personal suggestion this morning that we follow up with you and your staff about a technical matter involving the Health Insurance Portability and Accountability Act (HIPAA) electronic transactions standards as they impact the continued use of the Diagnostic and Statistical Manual of Mental Disorders (DSM). This matter is of urgent concern to the APA, and we deeply appreciate your willingness to review it.

As you know, HIPAA electronic transactions provisions that take effect in mid-October 2003 will mandate use of a single diagnostic code set (ICD-9-CM) for all disorders including mental disorders. As a result, in October 2003, the outdated 1977 ICD-9-CM "glossary of definitions and criteria" will become the only officially sanctioned diagnostic descriptors for ICD-9-CM codes. The 1977 ICD-9-CM descriptors do not represent current scientific understanding of mental illness. Because descriptors (text and diagnostic criteria) associated with ICD-9-CM mental disorder codes are outdated, by informal agreement DSM diagnostic criteria (currently published as DSM-IV) are used with ICD codes to define mental disorders in order to best ensure that the most recent descriptors (currently those in DSM-IV) are used, rather than the outmoded descriptors in ICD-9-CM.

Unfortunately, no provision has been made in law or regulation to permit the current informal agreement allowing for the use of DSM-IV descriptors (diagnostic criteria) to continue once the electronic transactions provisions of HIPAA go into effect in October. Unless action is taken to ensure the continued use of DSM-IV descriptors as long as ICD-9-CM is in use, we are concerned that DSM-IV descriptors will not be able to be used beyond the start date for the HIPAA electronic transactions requirements. Thus, practitioners may be required to use definitions and criteria for mental disorders that are more than 25 years out of date and do not represent current understanding of mental illness.

The DSM problem would be resolved if and when ICD-10-CM is implemented, since the current informal deferral by ICD-9-CM to DSM-IV would be officially codified in ICD-10-CM, in that under current draft ICD-10-CM criteria for mental disorders, the user is directly referred to DSM for definitions of mental disorders. In the meantime, however, action must be taken to ensure continued use of DSM-IV criteria.

Honorable Nancy Johnson
July 17, 2003
Page Two

APA has vigorously sought to ensure continued use of DSM criteria under the HIPAA rules throughout the regulatory process. In August, 2002, staff of the National Center for Health Statistics (NCHS) and the Centers for Medicare and Medicaid Services (CMS) recommended to the National Committee on Vital and Health Statistics (NCVHS) that Secretary Thompson issue a letter affirming that DSM-IV diagnostic criteria could continue to be used under HIPAA rules as descriptors for mental disorders in conjunction with ICD-9-CM diagnostic codes. Despite our efforts, to date there has been no action on the recommendation. Implementation of the HIPAA standards is now imminent, and we are running out of time to secure the recommended clarification through the administrative process.

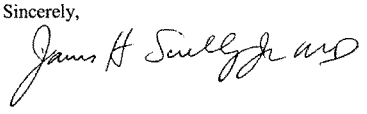
We believe the gap between use of ICD-9-CM under HIPAA standards effective in October and the point at which ICD-10-CM is fully implemented should be bridged by language in the Medicare reform bill or another appropriate vehicle specifying that the most recent DSM diagnostic criteria could continue to be used in conjunction with ICD-9-CM diagnostic codes under the HIPAA electronic transactions regulations. This could be accomplished quite simply through language that stipulated:

> **"To maintain consistency with current practice, the HHS Secretary will designate the most recent Diagnostic and Statistical Manual of Mental Disorders (DSM) diagnostic criteria as an official descriptor code set for the ICD-9-CM mental disorder codes."**

We recognize the difficulty in raising this issue at this time, but we are frankly hamstrung by the fact that there has been no decision one way or the other from HHS about whether they will retain the informal agreement permitting continued use of DSM-IV criteria once the HIPAA electronic transactions standards are implemented in October. Given the urgent need to ensure that all parties are able to use state of the art descriptors for mental disorders, we respectfully urge the Medicare conferees to include the simple language described above in the conference agreement on Medicare reform, or in some other appropriate legislative vehicle.

Thank you again for your willingness to consider this matter. We would be pleased to meet with you or appropriate members of your staff at any time.

Sincerely,



James H. Scully, Jr.
Medical Director

Testimony of the

American Psychiatric Association

on

Changes to the Medical Privacy Regulation

Before the

Health, Education, Labor, And Pensions Committee

U.S. Senate

Presented By

Richard Harding, M.D.

April 16, 2002

Mr. Chairman, and members of the Committee, I am Richard Harding, MD, testifying on behalf of the American Psychiatric Association (APA), a medical specialty society, representing more than 40,000 psychiatric physicians nationwide. I serve the APA as its President and am currently Professor of Clinical Psychiatry and Pediatrics at the University of South Carolina School of Medicine. In addition, I serve as Vice-Chairman for Clinical Affairs of the Department of Psychiatry and maintain a busy outpatient practice.

While I also serve on the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics within the Department of Health and Human Services (HHS), the views I am presenting today are my views and the views of the American Psychiatric Association.

First, I would like to thank Chairman Kennedy and the members of the Committee for the opportunity to testify today. My oral comments will be limited to two major concerns: consent and marketing. My written testimony is significantly more expansive as it reflects APA's comments on all of the NPRM privacy regulation changes, that we will formally submit to HHS, and I ask that it be made part of the hearing record.

Mr. Chairman we greatly appreciate your commitment to protecting medical records privacy. Privacy and particularly medical records privacy is an issue that not only affects all Americans but also one that they are deeply concerned about. On behalf of our profession and our patients I thank you for holding this hearing on the recent changes HHS made to the Medical Privacy Regulation.

While the Department of Health and Human Services (HHS) proposed HIPAA privacy regulation changes will reduce the burden on physicians and other healthcare providers, it is important to recognize they are inadequate to protect patients. The APA objects to the proposed elimination of the consent requirement that patients give written consent before their records are disclosed to physicians, hospitals or insurance companies. Under the proposed changes, consent is optional for direct treatment providers. HHS now gives their "regulatory permission" to allow a patient's information to be freely disclosed to health plans, providers, and clearinghouses without the patient's consent. The APA strongly believes patients should be able to choose who will see their medical records. The elimination of the consent requirement is a significant change not only to the historic doctor-patient treatment relationship but also an impediment to physicians' efforts to provide the best possible medical care. The consent requirement gave the physician the opportunity to discuss where their medical information would be released. We need to take steps to ensure that doctor-patient confidentiality is preserved and strengthened.

It is troubling to me as a practicing psychiatrist that a patient, under this rule, does not have consent authority over their medical records even if the patient pays out of pocket for their treatment. The proposed changes to the rule eliminate patient protection in a private payment situation with their provider by allowing information to be released without the patient's consent. For example, celebrities who seek help from a substance abuse center and pay in cash to be anonymous should be allowed to do so without their health information being released. Similarly, Medicare patients who elect to personally pay for treatment should not be at risk from the prying eyes of government.

Under the proposed changes, a privacy notice is substituted for consent. A privacy notice serves as a long and cumbersome notice that the records will be released. This is not privacy nor is it a protection of the patient's information. Furthermore, why must an ill patient have to look in the required privacy notice, which could be ten pages long as stated by the American Hospital Association. Buried within this lengthy notice is where a patient's medical information will be sent. As we have found out last week internet companies are selling a person's postal address and telephone number because the consumer did not notice in the long privacy notice that only e-mail addresses would not be released.

The APA recommends HHS retain the privacy rule's prior consent requirement, with targeted modifications to address the unintended implementation hurdles that result from the consent requirement in a couple of circumstances.

While the HHS proposed changes to the marketing provision appear to require an authorization from a patient before the patient receives marketing materials is well intentioned, the devil is truly in the details. The APA is concerned about the loopholes in the definitions of marketing through the enumerated exclusions from the appearance of protection by the so called marketing definition. There is no real effective privacy protection safety net against commercial usage of private patient information. Under HHS's changes, marketeers can use disease management, wellness programs, prescription refill reminders, case management and other related communications to send their marketing materials. These programs are not considered marketing. The regulations do not clearly restrict these marketing loopholes from abuses. It clearly is not in the best interest of the patient for a drug store to send a prescription refill reminder without the patient's authorization after the pharmacist was compensated by a pharmaceutical company. Recall not to long ago drug stores admitted to making patient prescription information available for use by a direct mail company and pharmaceutical companies. Now a pharmacy not only would be able to legally sell to a pharmaceutical company a list of patients that have been prescribed certain drugs in order to promote alternative drugs, but also the pharmacy could now in its own self financial interest in a medication's more profitable cost to them be suggesting a change in medication refill. The marketing communication would no longer need to identify the covered entity as the one making the communication, or need to state compensation was received.

Moreover, the fund raising provisions despite overwhelming testimony to the NCVHS urging that there be an "opt in" (prior consent) not "opt out" after the fact, using without permission an individual patient's name for the fund raising purposes of the covered entity. Can you imagine sending out millions of letters telling you the names of persons served in your substance abuse treatment program - -without their consent or authorization, and only thereafter, if the fund raiser wishes to do it again, then have to ask for the individual's permission to use her or his name in the fundraising endeavor. Does this sound reasonable to anyone.

I strongly urge the Committee to join us in requesting HHS require a patients consent and their authorization for marketing before their medical information is released under the Health Insurance Portability and Accountability Act (HIPAA). Also, in closing let me just briefly summarize our comments on parental rights to a minor's medical records, to

wit: there should be no changes to these provisions which have the effect of reducing access to health care by adolescent patients.

We thank you for this opportunity to testify, respond to your questions in continuing to work with the Committee on these important issues.

April 26, 2002

U.S. Department of Health and Human Services
Office of Civil Rights
Attention: Privacy 2
Hubert H. Humphrey Building
Room 425A
200 Independence Avenue, SW
Washington, D.C. 20201

RE: American Psychiatric Association Final Comments on Proposed Rule - Standards for Privacy of Individually Identifiable Health Information (Federal Register, March 27, 2002, PP14775-14814.)

Dear Secretary Thompson:

The American Psychiatric Association (APA), a medical specialty society representing more than 38,000 psychiatric physicians nationwide, believes the final privacy regulation is an important first step toward protecting patient privacy. However, we are concerned that additional protections are critically needed to protect patient privacy and to promote high quality health care, and such protections must be incorporated into the privacy regulation.

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 use your regulatory authority to respond appropriately in the public interest to protect the privacy of the medical record, and to achieve that result the APA urges the following revisions to the modification be made in the proposed regulations:

1) Section 164.506. Use and Disclosure for Treatment, Payment, and Health Care Operations.

Patients should be able to choose who will see their medical records. Under the Department's proposal, patient consent is eliminated for use and disclosure of medical information for treatment, payment, and health care operation purposes. This represents

not only a sea change to the historic doctor-patient treatment relationship, but also an impediment to physicians' efforts to provide the best possible medical care. We need to take steps to ensure that doctor-patient confidentiality is preserved and strengthened.

The right of consent is perhaps most important for those persons seeking and receiving mental health services. Mental health records can contain for the purpose of treatment particularly sensitive and potentially stigmatizing personal information if inappropriately disclosed. Considering the sensitivity of mental health records, patients should have the right to consent to their use and disclosure to insurers and other third parties.

While the Department of Health and Human Services' (HHS) proposed HIPAA privacy regulation changes will reduce the burden on physicians and other healthcare providers, it is important to recognize they are inadequate to protect patients. The APA objects to the proposed elimination of the patient consent requirement. Rather than have patients give written consent before their records are disclosed to physicians, hospitals or insurance companies, under the proposed changes, consent is optional for direct treatment providers. HHS has effectively given their "regulatory permission" to allow a patient's information to be freely disclosed to health plans, providers, and clearinghouses without the patient's consent. The APA strongly believes patients should be able to choose who has access to their medical records.

Currently and historically, physicians and hospitals obtain a patient's consent before treatment occurs and a patient's information is sent to third parties. We are deeply troubled a patient's consent would no longer be required. A consent form differs from the rule's proposed alternative, a notice form. The consent form is usually a page in length, and requests the patient's permission to send a patient's information to third parties. Conversely, a notice is much longer, and among the items buried in the fine print may be critical information, including the type of places where a patient's information may be sent. Additionally, the consent form triggers a conversation between a patient and the physician and allows the opportunity for the patient to inform the physician where they would like the information released.

Physicians have an ethical duty to seek a patient's consent. The written prior consent requirement should be restored, with exceptions for situations in which it is impractical or where it could have unintended consequences, for example, when a patient's information is needed to fill a prescription or schedule a referral, or to review previous treatment records so there will be no delay in treatment. This could be accomplished in a variety of ways. The patient's consent, appropriately noted in the patient's medical record, could be obtained orally or by fax. Physicians and other health care professionals can document oral consent – as they do today—where that occurs.

Alternatively, a pharmacist who receives prescriptions directly from doctors' offices, could be treated as an indirect treatment provider and not subject to prior consent. This could be accomplished through small changes to the definition of "indirect treatment relationship." Also in the first encounter situation prior to when a patient sees the physician to set up an appointment or schedule a surgery, the Department could create an exception to the written consent requirement when getting the patient's consent in advance is not reasonably practicable. Again, this could be premised upon an appropriate notation by the physician in the record.

Another of the issues of consent involves tracking revocation of consent. The Department can solve this issue by issuing guidance on what is "taking action in reliance thereon" of a patient's consent when the information is disclosed for health care operations like quality assurance studies.

In the circumstance where treatment is not provided in person to a patient or where doctors take phone calls for other doctors, the situation could be treated as part of an organized health care arrangement, with a joint consent form that authorizes use of the medical information in this way. Where there is an issue of nurses who staff telephone centers that provide advice over the phone, they do so under a contract with a health plan and are business associates of the health plan rather than separate covered entities subject to the consent requirement. Alternatively, a flexible oral consent option would obviate the difficulty here.

The Department could propose amendments to the emergency exception to alleviate emergency treatment providers' concerns that the emergency exception does not encompass all the activities in which they engage.

The Department has weakened the optional consent provision by "enhancing the flexibility of the consent process for those covered entities that choose to obtain consent." See 67 Fed. Reg. 14780. The APA is extremely concerned about a provision in the proposed regulation that "Consent of an individual under this paragraph shall not be effective to permit a use or disclosure of protected health information that is not otherwise permitted or required by this subpart." Added to this language should be an indication that it is limited to purposes of treatment, payment or health care operations. Although the preamble states that a consent voluntarily obtained by a provider or plan could not permit a use or disclosure that, according to other parts of the Privacy Regulation, requires an authorization, this is not stated explicitly in the actual text of the proposed regulation. See 67 Fed. Reg. 14781. If this language is not added to the regulatory text, a covered entity could substitute a consent form of its own design and choosing for an authorization that must meet certain specifications.

It is troubling that a patient, under this rule, does not have consent authority over their medical records even if the patient pays out of pocket for their treatment. The proposed changes to the rule eliminate patient protection in a private payment situation with their provider by allowing information to be released without the patient's consent. For example, public persons who seek help from a substance abuse center and pay in cash to be anonymous should be allowed to do so without their health information being released. Similarly, Medicare patients who elect to personally pay for treatment should not be at risk from the prying eyes of government.

Under the proposed changes, a privacy notice is substituted for consent. A privacy notice serves as a long and cumbersome notice that the records will be released. This is not privacy nor is it a protection of the patient's information. Furthermore, why must an ill patient be subjected to the required privacy notice, which as the American Hospital Association suggests, be as much as ten pages in length. Buried deep within this lengthy notice is the notice regarding where a patient's medical information will be sent, and it is not reasonable to expect the patient to seek out and find such information. Illustrative of

the problem is that Internet companies are selling a person's postal address and telephone number because the consumer did not notice in the long privacy notice the statement only e-mail addresses would not be released.

2) Section 164.501. and 508(a)(3) Standard: Uses and disclosures of protected health information for marketing and fundraising.

The APA is very concerned about the marketing and fundraising loopholes that exist in the regulation. While the Department's proposed changes to the marketing provision that appear to require an authorization from a patient before the patient receives marketing materials are well intentioned, the devil is truly in the details. The APA is concerned about loopholes in the definitions of marketing. An authorization requirement for marketing is only required for communications that encourage the purchase or use of a product or service that is not health related. The authorization requirement will not apply to communications that encourage the use or purchase of a health related product or service. These communications were excluded from the definition of marketing even though the covered entity is paid to make the communication. The Department also has changed the definition of marketing to exclude oral communications.

We are concerned that the exclusionary modifications have weakened the marketing section of the privacy regulation. Marketing loopholes were created for communications that encourage patients to purchase or use products or services that are health-related, including those that a covered entity is paid to make, which were removed from the definition of "marketing". Therefore, a pharmacist can sell a patient's prescription information to a different drug company with a more expensive alternative drug and receive compensation for the prescription list. The Mayo Clinic has recently announced a project to store in a database their patients' medical records, including their genetic information. Healthcare corporations will now be able to market to a targeted high-risk patient, even after the patient has left the organization.

Under the Department's changes, marketers can use disease management, wellness programs, prescription refill reminders, case management and other related communications to send their marketing materials. These programs are not considered marketing. The regulations do not clearly restrict these marketing loopholes from abuses. If a covered entity is receiving compensation from a third party, the patient should be informed so the patient can give his or her authorization to receive this information. There is no effective protection against commercial usage of private patient information.

It may not be in the best interest of the patient for a drug store to send a prescription refill reminder without the patient's authorization if the pharmacist is being compensated by a pharmaceutical company. We would suggest recalling that it was not too long ago that drug stores admitted to making patient prescription information available for use by a direct mail company and pharmaceutical companies. Now a pharmacy would be able to legally sell to a pharmaceutical company a list of patients who have been prescribed certain drugs. This allows marketers and pharmaceutical companies to promote alternative drugs and allows the pharmacy, in its own financial interest, to urge more profitable medications for their pharmacy on a patient by suggesting a change in medication. The marketing communication would no longer need to identify the covered entity as the one making the communication, or need to state that compensation was

received. A health plan would be able to sell the names of patients who have been prescribed certain drugs to a Pharmacy Benefit Manager to encourage promotion of alternative drugs or therapies.

Also, a health plan would be able to sell to a disease management company a list of patients with certain diagnoses to promote products or therapies that may save money for the plan. Patients should have the right to consent to - or refuse - participation in disease management or wellness 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 consent of the patient and coordination with and cooperation of the individual's physician. Yet, there is no such requirement in the proposed rule.

As mentioned above, mental health records are particularly sensitive to release and disclosure, due in part to the unfortunate stigmatization of mental disorders that continues to pervade society. A patient might not want his or her family, neighbors, or even postal delivery person to see a letter suggesting that he or she is on psychotropic medication. Such communications could undermine mental health care, as patients avoid or delay care in order to avoid stigmatization. We therefore urge rejection of the narrowing of the marketing definition to exclude communications that are financially motivated.

We strongly urge HHS to require a patient's authorization for communications encouraging the purchase or use of health-related products or services where the covered entity has received or will receive direct or indirect compensation. The Department should modify the provisions to require that an authorization for marketing specify whether the protected health information is to be used or disclosed for the marketing of health-care related services or products. HHS should include oral communications in the definition of "marketing". Also, a patient's authorization is not needed to make a marketing communication to a patient if it occurs face-to-face or it concerns products or services of nominal value.

Under the fundraising loophole, a covered entity may use or disclose a 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 that 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 communications. 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 the use of psychiatric patients 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 fundraising damage has occurred. There is an easy solution: merely require the fundraising endeavors to have a patient consent (opt in) before the activity occurs rather

than the regulation's authorizing the patient to opt out of any further fundraising endeavors.

3) Sections 164.506(c) Standard: Disclosures for treatment, payment, or healthcare operations of another entity.

With respect to healthcare operations, the Department proposes to permit a covered entity to disclose protected health information about a patient to another covered entity for certain healthcare operations purposes of the recipient covered entity. The activities that fall within the definition of health care operations and are permitted disclosures include quality assessment and improvement activities, population - based activities relating to improving health or reducing healthcare costs, case management, conducting training programs, and accreditation, certification, licensing, or credentialing activities, as well health care fraud and abuse detection compliance programs. The Department's definition of healthcare operations should include only those activities that are routine and critical for business operations and that can not be undertaken with de-identified information.

A covered entity would need to apply the minimum necessary provisions to both the disclosure of and request for information for payment and healthcare operations purposes. The Department clarifies this in the preamble and strongly encourages the use of de-identified information wherever feasible, but does not require it. However, we are concerned these provisions will place psychiatrist in an untenable position with respect to a determination of what is the minimum necessary information to disclose for a particular purpose. The APA recommends the language in the preamble on minimum necessary and de-identified information needs to be in the text of the regulation.

4) Section 164.502(b) Standard: Minimum Necessary.

We note that minor modifications to the "minimum necessary" requirement preserve the provision. Any future modifications or interpretations of this provision by HHS should ensure that the provision is interpreted most favorably to the patient, taking into account the treating physician's policies and procedures.

The "minimum necessary" requirement is of essential importance to the privacy of patient records. In essence, the privacy rule legitimizes a myriad of uses and disclosures for "treatment, payment, and health care operations" purposes beyond the patient and his or her direct treating providers. The minimum necessary requirement balances such broad access by ensuring that , for these purposes, the minimum amount of patient information will be disclosed in each instance. While we do not attempt here to offer specifics on the minimum necessary requirement, we believe that insurers should not request information for treatment, payment, or health care operations purposes absent a showing that they are requesting the minimum amount necessary for the purpose of their request.

We recognize and appreciate that the Department clarified that facility redesigns and expensive computer upgrades are not required. The Department reiterates in the preamble that covered entities may need to make certain adjustments to their facilities, as reasonable, to minimize access or provide additional security. Covered entities may decide to lock file cabinets or provide additional security, such as passwords on computers.

We are pleased the Department stated that it continues to believe that the privacy benefits of retaining the minimum necessary standard for these purposes outweigh the burdens. The APA urges HHS to retain the request for covered entities to develop minimum necessary policies and procedures.

Currently, only authorizations for disclosure to the individual are excepted from the minimum necessary standard. However, it is not clear why this exception should be expanded to include all authorizations for any purpose, simply because there will only be one uniform set of requirements for the content of an authorization. This is of concern for authorizations pertaining to psychotherapy notes. Therefore the APA believes that HHS should retain the minimum necessary standard for disclosures pursuant to an authorization other than disclosures to the individual, and that the exception to the minimum necessary standard in Section 164.502(b)(2) should be specifically limited to disclosures to an individual.

5) Section 164.508 Uses and disclosures for which an authorization is required.

The APA supports the Department's efforts to simplify the authorization provision, however the minimum necessary provisions should remain applicable to any uses and disclosures of protected health information. We urge the Department to retain the core elements required for research authorizations involving treatment of an individual under the privacy regulation, require remuneration disclosures in all authorizations, not only in authorizations for marketing, and retain the plain language requirement as a core element of a valid authorization.

The APA commends the Department for tightening the provisions on the use and disclosure of psychotherapy notes without authorization to carry out treatment, payment and healthcare operations. See proposed Section 164.508(a)(2)(I)(A), (B), and (C). We strongly support the Department's proposal to clarify that psychotherapy notes may not be used or disclosed without individual authorization for another entity's treatment, payment and healthcare operations purposes. 67 Fed. Reg. 14798.

The APA is concerned that in an effort to streamline the authorization process the Department is proposing to remove critical elements from the authorization. The privacy regulation currently requires an authorization to include what information will be used or disclosed, by whom, to whom, the purpose of the use or disclosure, an expiration date or event, and the individual's signature and date, information about revocation and notice of the potential for redisclosure. However, there are also other requirements specifically for three types of authorizations. The Department proposes to consolidate these authorizations under one set of criteria.

It is critical that an individual know how his or her research – related information will and will not be used or disclosed so that he or she can make an informed decision about giving authorization. Patients may not want their insurers to know about their participation in the study or about the treatment they will be receiving. It is critical that individuals are informed of a provider/researcher's monetary interests in obtaining the individual's authorization. The plain language requirement is critical to ensuring that an

individual's authorization is informed and voluntary so it is understood by the average reader.

6) Section 164.502(g)(3) - Implementation Specification: Unemancipated Minors (67 Fed. Reg. 14811-14812).

While we are disappointed with one aspect of section 164.502(g)(3) of the proposed rule, we are pleased overall that the proposal for this section recognizes the critical role of health care providers in determining when protected health information concerning a minor may be disclosed and allows health care professionals to honor their ethical obligations to protect minors' privacy in important circumstances. In doing so, the proposed regulation preserves some key aspects of the relationship between health care professionals and their minor patients. This is a commendable aspect of the proposed rule.

However, the proposed modifications do not preserve the same level of privacy protection for minors as in the current Privacy Rule. The current Privacy Rule acknowledges that state and other laws recognize minors' competence to consent to health care services and allow them to do so in a range of circumstances in order to encourage them to seek care. The current Privacy Rule also acknowledges the established clinical practice in which parents of minors assent to an agreement of confidentiality between a minor and a health care professional. In both of those circumstances, the current Privacy Rule allows minors to act as "the individual," with control over and access to their own protected health information.

While the proposed modifications maintain this basic framework, they also allow health care providers to overrule minors' privacy in circumstances not allowed by the current Privacy Rule. Although it is necessary and appropriate at times for the health care provider to inform parents or guardians of certain health problems facing a minor, the proposed regulations represent a loss for minors in determining who may have access to their protected health information. Any further erosion of the privacy protection provided for adolescents would seriously undermine the likelihood that they will seek necessary care and the ability of health care providers to provide appropriate care while honoring their ethical obligations.

Under proposed new Section 164.502(g)(3)(i), when a parent is authorized to make health care decisions for an unemancipated minor child, including an adolescent, the parent would be the "personal representative" of the minor and would have access to and control over the protected health information relating to the minor's health care, except in specified circumstances.

Specifically, under proposed new Section 164.502(g)(3)(i) (A), (B), or (C), when an unemancipated minor is authorized to consent for his or her own health care or when a parent has assented to a confidentiality agreement between a health care provider and a minor, the minor is allowed to exercise the rights as an individual with respect to his or her own protected health information and the parent may not do so. This basic framework is an essential element of encouraging adolescents to seek care for problems such as substance abuse and mental health concerns: it should be maintained in the final rule.

Under proposed new Section 164.502(g)(3)(ii)(A), if state or other law explicitly requires disclosure of protected health information to a parent, the rule does not prevent a health care professional from complying with the requirement; and, if state or other law explicitly permits disclosure of protected health information to a parent, a health care professional would have discretion to determine whether or not to disclose the information to a parent.

Under proposed new Section 164.502(g)(ii)(B), if state or other law explicitly prohibits disclosure of protected health information to a parent, a health care professional would not be permitted to disclose it. This approach - of deferring to decisions by states to authorize or prohibit disclosure of information to parents - is contained in the current Privacy Rule: in the proposed new rule, it has been moved from the section on preemption (Section 160.202(2)) to this section. This continues to allow the current practice, which some states have adopted in their laws, of giving health care professionals the discretion to determine whether or not to disclose protected information about a minor's care to parents, even when the minor has consented to the care. That discretion is limited only if a state explicitly acts to do so.

As stated in the preamble to the new rule (67 Fed. Reg. 14791-14793), proposed new Section 164.502(g)(3)(iii) specifies how access to protected health information for a minor is to be handled when state or other law is silent or unclear on parental access. This provision would apply when the minor is allowed by the rule to act as "the individual" and the parent is not " the personal representative" of the minor because the minor has the right to give his or her own consent for care or the parent has assented to a confidentiality agreement. In these circumstances, a health care professional would have discretion to determine whether to give access to the protected health information to a parent, to the minor, or to both. The preamble makes clear that the "proposed language would not require a provider to grant access to a parent." (67 Fed. Reg. 14792). However, access would have to be given either to the minor, to a parent, or to both, and could not be completely denied (except in limited circumstances allowed by other sections of the rule).

In granting discretion to health care professionals when state or other law is silent, proposed new Section 164.502(g)(3)(iii) uses the term "covered entity." We believe that the proposed new rule should be modified to use the term "covered health care provider who is a licensed treating health care professional." In explaining this section of the proposed new rule, the preamble uses the term health care provider and clearly contemplates that the decision about whether or not to provide parents with access to protected health information about a minor who is allowed to give his or her own consent to care will be made by a health care professional who has a relationship with the adolescent. It would be inappropriate for such sensitive determinations that require the exercise of professional judgment to be made by the broad array of individuals and groups encompassed by the term "covered entity" and we believe the proposed new rule intended such determinations to be made by health care professionals.

In conclusion, the proposed modification to Section 164.502(g)(3) clearly represents an effort to achieve a balance between the parents' access to medical records of their children and the ethical obligations that health care providers have in providing care to their minor patients. This equilibrium contained in the proposed rule continues the basic approach of the current Privacy Rule, while limiting minors' privacy in favor of granting

greater discretion to health care professionals. Any changes to the medical privacy regulations that further limit minors' privacy would seriously impede our ability as health care professionals to deliver the best care to our minor patients and to ensure that they seek care when necessary. We would view this as a disastrous reversal of the current and proposed approach to delivering health care to minors that has been developed over many decades and that works well.

7) Section 164.502 (a)(1)(iii) Uses and disclosures of protected health information: Oral Communications.

The Department proposes that an incidental use or disclosure would be permissible only to the extent that the covered entity has applied reasonable security safeguards, and implemented the minimum necessary standard, where applicable. This was in response to concerns about using sign-in sheets in waiting rooms, maintaining patient charts at bedsides, whether X-ray light boards will need to be isolated, or whether empty prescription vials will need to be destroyed.

We are pleased that under this proposal, an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, is a violation of the privacy regulation. A covered entity that asks for a patient's health history on the waiting room sign-in sheet is not abiding by the minimum necessary requirement.

Also, the proposal does not intend to excuse erroneous uses or disclosures that result from mistake or neglect in the absence of reasonable safeguards. An impermissible disclosure would occur when a covered entity mistakenly sends protected health information via electronic mail to the wrong recipient.

8) 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 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. 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. The concept of scalability should be expanded so that the administrative burden on physicians in solo or small practices will be manageable, taking into consideration their limited resources and staffing.

The APA opposes the Business Associate provisions as representing overly broad physician liability. However, we appreciate the one-year extension to modify current contracts to comply with the Business Associate provisions. We also appreciate the Department's attempting to provide form language for the business associate agreement, but regulatory language is not appropriate as contract language. The model language would not eliminate the need for state legal assistance in preparing and negotiating these contracts and the cost and burden remains.

9) Section 164.514 Standard: de-identification of protected health information.

The APA commends the Department for not changing the de-identification provisions of the privacy regulation. We urge the Department to continue to maintain these provisions in the privacy regulation. We are especially concerned about the de-identification of the birth date and zip codes in small communities and rural areas.

10) Section 164.520 (a)(2) Exception for group health plans.

The proposed changes clarify that group health plans may disclose enrollment and disenrollment information to plan sponsors. This disclosure is permitted even if the plan documents have not been amended to specify how that information will be used and to whom it will be disclosed. Employers with self-funded health plans may need information that goes beyond enrollment and disenrollment information or summary information. We believe plan documents need to be amended before such disclosure takes place.

Many employers with self-funded health plans have contractual arrangements with third parties to provide services relating to plan administration. The proposed changes to the business associate provisions in the privacy regulation will have an impact on a health plan's contracts with its business associates. A significant aspect of the proposed changes for employers involves employment records. The proposed changes would clarify that "employment records held by a covered entity in its role as employer" are not protected health information. The proposed change makes clear that a covered entity, such as a hospital, would not have to treat employment records, such as drug test results, OSHA records, workplace medical surveillance, and fitness for duty paperwork, as PHI. We believe that employment records should not include this information, as an employee can be discriminated against by losing their job based on this information, and that if it is included, it should be treated as protected health information.

11) Section 164.528 Accounting of disclosures of protected health information.

The privacy regulation allows individuals the right to obtain an accounting of disclosures of PHI made by covered entities, with certain exceptions. Such exceptions include disclosures made by covered entities for treatment, payment or health care operations, and disclosures to individuals of PHI about them. We do not agree with the exceptions under the accounting requirements in Section. 164.528 to include disclosures made in authorizations under Section 164.508 (Psychotherapy notes). We disagree with the Department's position that accounting disclosures are unnecessary since the individual should already be aware of the disclosures and the individual was required to sign forms authorizing the disclosures. A patient should always have the right to monitor access to their personal information.

12) Section of 164.504 Uses and disclosures: organizational requirements.

The APA is concerned about the Department's revising the definition of "hybrid entity" to significantly broaden the use of this designation. The privacy regulation introduced the concept of "hybrid entity" to describe a single legal entity that engages in both covered functions and non-covered functions. The Department proposes to delete the word "primary" from the definition of hybrid entity and to permit any covered entity to designate itself as a hybrid entity as long as it is a single legal entity that performs both covered and non-covered functions. A hybrid by this definition would exist regardless of whether the non-covered function represents that entity's primary function, a substantial function, or a very small portion of the entity's activities. This change would appear to greatly increase the number of covered entities that are hybrid entities and makes treatment as such dependent on the needs of the entity and not on the interpretation of the word "primary."

Covered entities would be free to weigh the advantages and disadvantages of the designation and choose whether to treat the entire entity as a covered entity or just the healthcare component. The Department modified the definition of healthcare component slightly to allow the hybrid entity to designate as the healthcare component any sections of its business that it chooses. At a minimum though, it must include those components that would meet the definition of a covered entity if they were separate, stand-alone legal entities. The hybrid entity, therefore, would not be required to designate a component that is a healthcare provider, but does not engage in standard electronic transactions.

Disclosures of PHI between the healthcare component of the hybrid entity and the remainder of the entity would be treated just like any other disclosure by a covered entity to a non-covered entity. Such disclosure would violate the privacy regulation unless permitted or required under some other section of the privacy regulation or where the hybrid entity obtains an authorization. The components of a hybrid entity that provide services to the component that performs covered functions (e.g., legal or accounting department) may be included in the designation of the healthcare component so that PHI can be shared with them without the necessity of obtaining individual authorizations or business associate agreements.

To avoid needless application of hybrid entity provisions to a covered entity's activities as an employer of its own employees, the Department modified the definition of PHI to exclude employment records held by the entity in its role as employer of its own employees. This change will limit the need for a covered entity to designate itself as a

hybrid entity just to carve out its own employment records. We believe the term employment records is not clear and needs to be further defined.

The APA rejects the proposal that any covered entity can elect to be a hybrid entity, and that allows those covered entities whose primary functions are not covered functions to be hybrid entities and to erect firewalls between their health care components and other components. We recommend that you modify the implementation specifications of the proposed modified hybrid provisions to require that a hybrid entity must designate a component that performs covered functions as a health care component.

The Department needs to clarify that a health care provider (including a component of a hybrid entity that provides health care) cannot avoid being deemed a "covered entity" if it relies on a third party to conduct its standard electronic transactions. Also, clarify that with respect to hybrid entities, a health care provider cannot avoid having its treatment component considered a health care component by relying on a billing department to conduct its standard electronic transactions.

13) We welcome your retaining the positive provisions contained in the regulation and urge that they remain , including:

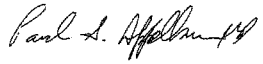
- the general rule of non-preemption of more privacy protective state laws (Section 160.203)
- a higher level authorization requirement for any use or disclosure of psychotherapy notes, and most importantly that psychotherapy notes may not be disclosed without the patient's specific authorization (Section 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" requirement. 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 an 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 requirement that 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. We

firmly believe that these regulations must put the patient first and then seek to build enhancements to the business model.

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,



Paul S. Appelbaum, MD
President-Elect

News RELEASE

American Psychiatric Association, 1400 K St. NW, Washington, DC 20005

For Information Contact:
Julie Abadie, 202/682-6056
JAbadie@psych.org

Nancy Trenti, 202/682-6046
NTrenti@psych.org

August 13, 2002
Release No. 02-27

APA Disappointed with Final Changes to HHS Medical Records Privacy Rule

Statement by Paul S. Appelbaum, M.D.
President, American Psychiatric Association

The American Psychiatric Association (APA) is deeply disappointed with the final Department of Health and Human Services' (HHS) changes to the HIPAA privacy regulations. In their ultimate form, HHS's privacy rules abandoned patients' fundamental right of prior consent to the disclosure of personal medical information. Abolishing the prior consent requirement regrettably will ensure that patients no longer have control over who has access to their medical records. As a result of this action, patients may be discouraged from revealing information to their physicians that is necessary for their treatment. Additionally, physicians may be encouraged not to record important but embarrassing or deeply personal information in their patients' medical charts out of concern for their patients' privacy. We are also worried that there are inadequate protections against the disclosure of patients' medical information in circumstances that could lead to the loss of employment or insurance.

The APA has been in the vanguard of defending patients' medical record confidentiality and historically has advocated forcefully before the Congress and the Executive Branch for patients' right to prior consent to the use and disclosure of their personal medical information.

The Bush Administration's decision on regulations governing the marketing of medical information is also troublesome. According to the Administration's own account, they have created a loophole whereby a pharmaceutical company will be permitted to pay a pharmacy to recommend to patients that they switch from one medication to another, and there will be NO requirement to disclose this arrangement to patients. Moreover, patients will be unable to decline to receive such solicitations. This unwarranted interference with the patient/physician relationship is not justified by any benefit to patients, but is motivated solely by the economic interests of the pharmaceutical industry.

To be sure, there are positive aspects to the regulations, including some restrictions on the sale of patients' medical information, and increased rights of patients to see and correct errors in their records. In addition, the final regulation maintains the requirement for specific patient authorization for release of psychotherapy notes, with limited exceptions. But the value of these positive measures is seriously compromised by the retreat on patients' rights to determine what happens to their records and to prevent their information from being used for commercial purposes.

It is interesting to note that the Administration did not publish the full text of the privacy regulations; rather, it only published the modifications to the previous regulations issued during the closing days of the Clinton administration. The Administration's decision to publish these landmark regulations in this fragmented format evokes our concern that such publication fails to provide clear and sufficient guidance to the American public. It is our hope that the issuance of these important modifications late on a Friday in August,

in a form that makes their significance difficult to judge, will not preclude public debate over the choices that have been made and the ways in which patients' interests have been sacrificed.

The American Psychiatric Association is a national medical specialty society, founded in 1844, whose 38,000 physician members specialize in the diagnosis, treatment and prevention of mental illnesses including substance use disorders. For more information, visit the APA Web site at www.psych.org.

American Psychiatric Association

1400 K Street, N.W.
Washington, DC 20005
Telephone: 202.682.6046
Fax: 202.682.6287
E-mail: ntrenti@psych.org
Internet www.psych.org

TESTIMONY

of the

AMERICAN PSYCHIATRIC ASSOCIATION

on the

MEDICAL PRIVACY REGULATION

before the

SUBCOMMITTEE ON HEALTH

of the

ENERGY AND COMMERCE COMMITTEE

U.S. HOUSE OF REPRESENTATIVES

Presented by

PAUL APPELBAUM, M.D.

MARCH 22, 2001

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 implementation 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. 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.

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 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.

American
Clinical Laboratory
Association

Statement of the
American Clinical Laboratory Association
to the United States Senate
Special Committee on Aging
on the HIPAA Standards for Electronic Transactions

The American Clinical Laboratory Association ("ACLA") is pleased to have the opportunity to submit this statement regarding implementation of the HIPAA Standards for Electronic Transactions ("transaction standards") to the Committee. ACLA is an association representing independent clinical laboratories throughout the United States including local, regional and national laboratories. In the United States alone, clinical laboratories perform millions of tests each year for physicians and other health care professionals. Virtually all of the billing for this testing is done electronically. Thus, ACLA members will be significantly affected by the implementation of the transaction standards. More importantly, the difficulties faced by clinical laboratories are being felt across the health care industry and will ultimately have an impact on patients.

Background

Congress's stated purpose in enacting HIPAA was to increase efficiency and reduce the costs of health care administration by facilitating electronic billing and payment for the provision of health care. To accomplish this goal, the transaction standards require that electronic health care transactions submitted by most health care providers and clearinghouses meet new format and content specifications. This means that most providers are now being required to obtain a variety of new data elements, which they were previously not required to obtain, and which have historically not been necessary for payers to adjudicate health care claims. These new requirements for claims processing will place a tremendous burden on clinical laboratories and other covered entities that may not have access to the required information.

As the compliance date for the transaction standards draws nearer, there are increasing concerns throughout the health care industry about the possible adverse impact on the health care system from implementation of the standards. In fact, it appears that the Department of Health and Human Services' ("HHS") current interpretation of some HIPAA requirements actually will increase – rather than reduce – the administrative complexity of the health care billing and payment process. In addition, there are serious doubts about the efficacy and fairness of the established regulatory processes for future maintenance and update of the standards. Although ACLA members are committed to compliance with the transaction standards, ACLA believes that HHS must provide more specific guidance to assist providers struggling with implementation and must streamline the mechanisms for development and maintenance of the transaction standards.

Unique Difficulties Experienced by Clinical Laboratories

Clinical laboratories are in a unique position with respect to implementation of the transaction standards because they typically have no contact with the patient, and therefore, have

1250 H Street, N.W. • Suite 880 • Washington, DC 20005 • (202) 637-9466 Fax: (202) 637-2050

no opportunity to obtain much of the new required information. Clinical laboratories generally perform testing at the request of a physician, on a specimen they pick up from the physician, and they report test results back to the same physician. As a result, clinical laboratories must rely upon physicians to provide patient information. However, because of other demands on their time and the time of their staffs, physicians routinely fail to provide such information to the laboratory, even when the laboratory specifically and repeatedly requests the information. Thus, the unique role of the laboratory as an indirect treatment provider creates additional complexity for the laboratory's efforts to comply with the transaction and code sets standards.

Since the laboratory generally does not see the patient, the data elements that are most problematic are those that require demographic information that is usually supplied by the patient. For instance, obtaining patient name, address, and date of birth, and subscriber name, address, and date of birth is often difficult, if not impossible, for a laboratory. Accordingly, ACLA has requested changes related to these data elements, as well as to the diagnosis information, referring provider identification, and responsible party data elements, through the appropriate processes. ACLA believes that these requested changes are necessary to streamline the claims processing system for physicians, payers, and laboratories alike.

Diagnosis Codes as an Example

The diagnosis code data element serves as good illustration of the difficulties faced by clinical laboratories in acquiring the information necessary to submit claims in compliance with the transaction standards. Currently, clinical laboratories are only required to provide a diagnosis code on claims in limited circumstances. The laboratory negotiated rulemaking proceeding, which was required by the Balanced Budget Act of 1997, established requirements for clinical laboratory billing and documentation. The negotiated rulemaking process brought together all of the stakeholders involved in clinical laboratory testing, including laboratories, physicians, and the government itself. As a result of that process, it was agreed that diagnosis codes would not be required on all laboratory claims. In fact, when CMS issued the rule resulting from the negotiated rulemaking, it concluded that requiring diagnosis information on all claims would "present significant burdens on some physicians" and laboratories. *See* 66 Fed. Reg. 58788, 58791 (Nov. 23, 2001).

As a result, the Medicare Program has only required laboratories to have diagnosis codes in narrow circumstances (*e.g.*, testing that is covered by a national coverage decision, or a local medical review policy). *See* Medicare Carriers Manual § 2010.2 (Item 21). However, the current Implementation Guide for the transaction standards requires the diagnosis code element on all claims/encounters except claims for which there are no diagnoses (*e.g.*, taxi claims). ACLA believes requiring diagnosis information on health care claims creates an unreasonable burden on clinical laboratories because they cannot supply diagnosis codes on their own.

Laboratory testing is furnished by laboratory technicians and technologists, who, though highly skilled in performing these tests, are not trained or licensed to make a diagnosis. Most importantly, the laboratory claim does not contain a diagnosis rendered by the laboratory; all the laboratory can do is pass on the information received from the ordering physician. It is the physician – not the laboratory – who actually diagnoses the patient. Indeed, under federal fraud

and abuse laws, laboratories may be sanctioned for using diagnosis codes (ICD-9 codes) that are not supplied by the physician or his or her staff. *See* Office of Inspector General Compliance Program Guidance for Clinical Laboratories, 63 Fed. Reg. 45076 (August 24, 1998). As a result, clinical laboratories must rely upon physicians to provide diagnosis information. However, physicians often object to having to list ICD-9 codes for individual tests, and even when laboratories specifically request diagnosis information, physicians routinely fail to provide it.

ACLA believes that requiring diagnosis codes on laboratory claims places the burden of obtaining the information on the party least likely to be able to obtain it. Physicians have little incentive to provide the laboratory with diagnosis codes because there are virtually no legal or financial consequences to the physician for transmitting incomplete information to the laboratory. The laboratory has no ability to force the physician to turn over this information if he or she fails to provide it in the form required to submit the claim or at all. In the process, the laboratory is forced to expend precious resources as it repeatedly, but unsuccessfully, attempts to obtain the information from the physician.

As a practical matter, the laboratory cannot refuse to perform testing ordered by a physician. Laboratory testing is a critical, and often time-sensitive, health care service. Most laboratories feel they are obligated to perform the testing that is ordered once they receive a specimen and the laws of several states specifically require testing on all specimens that are submitted to a laboratory. Further, a laboratory could be held liable if the patient later suffered harm as a result of the laboratory's failure to perform testing ordered by a physician. Thus, the practical reality is that if diagnosis information is required to electronically submit a claim, laboratories will be faced with filing paper claims or will end up doing testing for free when they cannot obtain the required information from the physician.

Furthermore, in most circumstances, diagnosis information has no bearing on the processing of the claim for payment. In fact, many of the data elements that are required by the Implementation Guide are not being used today by payers to process claims. For instance, in the encounter setting – where the payer agrees to pay the laboratory a bundled or capitated amount per month for the testing provided – there is no need for such information. Consequently laboratories have no system in place to capture diagnosis information for testing reimbursed in this manner. The reality is that many other third party payers do not require this information to adjudicate claims.

The requirement for diagnosis information provides a good illustration of the difficulties being experienced by covered entities as they attempt to comply with the new transaction standards. These difficulties are being felt across the health care industry. As a result, ACLA has been working with a coalition of health care providers, clearinghouses, and payers to help establish consensus on the problematic aspects of the standards and work toward mutually agreeable resolution of these issues. The coalition's efforts to work through these troublesome issues have revealed the problems inherent in the regulatory process that governs the transaction standards.

The Unworkable Regulatory Process

The HIPAA statute generally requires HHS to adopt a standard that has been developed, adopted, or modified by a standard-setting organization. However, the statute also requires that any standard adopted be consistent with the objective of reducing the administrative costs of providing and paying for health care and accommodate the needs of different types of health care providers. To comply with the directives in the statute, the transaction standards regulation published in the Federal Register on August 17, 2000 established a new category of organization, the "Designated Standards Maintenance Organization" ("DSMO"). The regulation provides that the Secretary may designate as DSMOs those organizations that agree to maintain the standards adopted by the Secretary. These organizations maintain the standards for health care transactions adopted by the Secretary, and receive and process requests for adopting a new standard or modifying an adopted standard. Currently, there are six DSMO organizations. In addition, there are three advisory bodies that HHS must consult with regarding the transaction standards, including the Workgroup for Electronic Data Interchange ("WEDI") and the National Committee on Vital and Health Statistics ("NCVHS").

The challenges faced by clinical laboratories in securing all data elements required to submit a compliant standard transaction are tremendous. As we have explained, this is largely due to the fact that the laboratory does not typically see the patient and must rely on another provider to pass along the information. To address these concerns, ACLA and its members have attempted to participate to the fullest extent possible in the designated regulatory processes for discussion of and revisions to the transaction standards. ACLA has submitted a formal change request to the DSMOs to address the problematic data elements. In addition, ACLA has submitted testimony about its concerns to the NCVHS Subcommittee on Standards and Security. Recently, ACLA also submitted comments on the draft ANSI ASC X12N 4050 Implementation Guide for the Professional Health Care Claim, and ACLA members regularly participate in these individual DSMO organizations' meetings and activities. ACLA has also developed an educational document to assist its members in notifying physicians about the new requirements for additional information on health care claims. We have attached this document to our statement for your reference. Finally, ACLA has met repeatedly with officials at HHS to discuss these issues.

Based on these experiences, ACLA has serious concerns about the accountability and efficacy of the regulatory processes for creating and revising the transaction standards. The DSMO process moves very slowly and has no ability to make changes to the current standard created by the standard setting organization and adopted by the Secretary. According to the DSMO member organizations, the change request process can affect only future versions of the transaction standards, and this is likely to take many years. In the interim, covered entities have no ability to obtain necessary modifications to the standards. In addition, the DSMO organizations are private, standard-setting bodies, which have historically enjoyed more participation from the payer community. Only since HIPAA mandated the adoption of a standard developed by these organizations have providers needed to become involved in their activities; consequently, there is still much work to be done in educating the individual DSMOs about the issues faced by providers. Moreover, since these are private standard-setting bodies,

○