



GEORGETOWN UNIVERSITY

Institute for Health Care Research and Policy

## **Testimony before the**

### **National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality**

### **Implementation of the Federal Standards for Privacy of Individually Identifiable Health Information**

**Joy L. Pritts, J.D.**  
**Senior Counsel, Health Privacy Project**  
**Research Assistant Professor**

**October 30, 2002**

**Mr. Chairman, Members and Staff of the National Committee on Vital and Health Statistics, Subcommittee on Privacy and Confidentiality:**

Thank you for the opportunity to testify before you today on issues related to the implementation of the medical privacy rule issued under the Health Insurance Portability and Accountability Act of 1996 (the “HIPAA Privacy Rule” or the “Privacy Rule”). I am Joy Pritts, Senior Counsel for the Health Privacy Project and a Research Assistant Professor at Georgetown University’s Institute for Health Care Research and Policy.

In my position at Georgetown, I conduct research and analysis on a range of health privacy issues. The HIPAA Privacy Rule and its interaction with state health privacy laws has been a particular focus of mine. I am the primary author of *The State of Health Privacy* (1999), a comprehensive compilation of major state health privacy statutes, which is currently being updated, and the author of *Implementing the Federal Health Privacy Rule in California* (2002), a set of introductory guides for practitioners, health plans, and pharmacists describing the interaction of the HIPAA Privacy Rule and California law. My article, “Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule,” was recently published in the *Yale Journal of Health Policy, Law, and Ethics* (Spring 2002).

For over 40 years, state law has provided the primary legal protections for the privacy of medical information. The promulgation of the HIPAA Privacy Rule significantly alters this legal landscape. The HIPAA Privacy Rule is the first – and only – federal law to protect the privacy of medical information in the hands of private health care providers and health plans. It will set a minimum standard of privacy protection across the nation and constitutes a step toward restoring the public trust and confidence in our nation’s health care system. But the benefits of this federal law will only come to fruition if the Privacy Rule is implemented in comprehensive and timely fashion.

In very general terms, the HIPAA Privacy Rule creates a federal “floor” of privacy protection. While the Privacy Rule generally preempts contrary state laws, it permits contrary state laws that are “more stringent” than the Privacy Rule to remain in place. A critical step in implementing the HIPAA Privacy Rule is determining the precise manner in which the federal rule interacts with state laws and with other federal laws (*i.e.*, conducting preemption and implied repeal analyses). This process of determining what laws are preempted (or repealed) and what laws remain in force must be undertaken before covered entities can establish privacy policies, procedures, and training to fully comply with both federal and state standards.

My testimony today will address implementation issues surrounding preemption and implied repeal analyses and possible steps that can be taken to facilitate these analyses. As requested, I have focused my discussion on issues that affect small provider groups and sole practitioners.

## I. PREEMPTION ANALYSIS: AN ARDUOUS PROCESS

The framework for preemption of state laws under HIPAA is complicated. In general, the HIPAA Privacy Rule preempts contrary provisions of state law, *i.e.*, those where a covered entity would find it impossible to comply with both the state and federal law or where the provision of state law stands as an obstacle to the accomplishment and execution of the goals of the Privacy Rule. However, contrary state laws that are “more stringent” than the HIPAA Privacy Rule are *not* preempted. With respect to patient access, the federal rule defines the term “more stringent” generally as meaning that the state provision provides a person with greater rights of access to his own health information. With respect to uses and disclosures, the term means that the state law prohibits or restricts a disclosure that would be allowed under the federal rule. Additionally, HIPAA does not preempt certain state laws that relate to public health.<sup>1</sup>

In light of this framework, conducting a preemption analysis is an arduous process. Although there are a number of different approaches to preemption analysis, all of them require comparing state laws to the HIPAA Privacy Rule on a provision-by-provision basis. This presents a number of challenges.

### *Lack of Familiarity with Applicable Laws*

A key element to conducting a preemption analysis is identifying the relevant state laws that are to be compared with the HIPAA Privacy Rule. Reduced to its most basic elements, preemption analysis requires knowledge of the laws that are to be compared. Many covered entities lack familiarity with their state’s applicable health privacy laws.<sup>2</sup> This presents a basic obstacle to undertaking a preemption analysis. One of the positive consequences of the HIPAA Privacy Rule is that it is forcing covered entities to review and become knowledgeable about their state privacy laws.

The other side of this equation, of course, is the requirement that a covered entity be thoroughly familiar with the requirements of the HIPAA Privacy Rule. Although many providers appear to be acquainted with the HIPAA transaction requirements, the HIPAA Privacy Rule is only now appearing on their “radar screen.” A preemption analysis simply cannot be done without a thorough knowledge of the federal regulation.

Even those who are knowledgeable of the HIPAA Privacy Rule have difficulty interpreting how some of the provisions apply to specific situations. Some of this confusion results from the ambiguous language of the federal rule. For instance, the provisions of the HIPAA Privacy Rule that permit disclosures without a patient’s

---

<sup>1</sup> The HIPAA Privacy Rule also contains a carve-out that preserves state laws that require health plans to report or provide access to certain information for specified purposes such as management audits.

<sup>2</sup> Covered entities are not necessarily violating state law. Many covered entities realize that they must (or must not) undertake certain actions but are not familiar with the legal basis for their actions.

permission for public health purposes generally limit those disclosures to a public health authority that is “authorized by law” to collect the information. One provider group queried whether this phrase required the activity to be within the general purview of the public health authority or required the activity to be specifically authorized in a statute or regulation.

### *The Appropriate Level of Comparison Between State and Federal Law*

Another key issue that must be addressed in a preemption analysis is how narrowly to construe a “provision” of state law. A “provision” is clearly narrower than a section, or even a subsection, of a statute. But determining the appropriate breadth of comparison can be difficult. Attachment A shows an example of a comparison of California and federal provisions that allow a provider to deny a patient access to his own health information. The subsections of law are broken down into the following provisions: type of health information to which access can be denied; who is entitled to make the determination to deny access; the standard of risk to be imposed in making the determination; and whose endangerment justifies denial (patient or other person). Both the state and federal subsections addressing denial of access are fairly short, yet four separate provisions must be compared in the preemption analysis.

I would like to point out that the level on which a preemption analysis must be undertaken is an area of frequent misunderstanding. Some providers and their professional organizations are under the misperception that the state-federal law comparison is made on a very general basis, *i.e.*, that they do not need to look at specific provisions of law, but only make a general comparison. If their state laws are generally strong, they believe their state laws will not be preempted by HIPAA. Being advised that this approach is erroneous and that they need to do a provision-by-provision analysis is a rude awakening.

We have encountered similar misunderstandings with those who are trying to comply with the HIPAA Privacy Rule and other federal laws. One clinic told us that they were informed by a state agency that they need not comply with the HIPAA Privacy Rule as long as they complied with the federal confidentiality of substance abuse regulations since the latter are more stringent than HIPAA. This recommended global approach to implied repeal analysis is inappropriate.

### *Comparing Apples to Oranges*

Another difficulty in conducting the preemption analysis is the fact that many of the provisions in the HIPAA Privacy Rule do not have directly comparable provisions in state law. Many of the general provisions governing patients’ access to their own health information can be directly compared. However, comparing state and federal provisions that restrict use and disclosure is a more difficult process because the provisions are structured differently and use different terminology. For example, the HIPAA Privacy Rule permits the use and disclosure of health care information without the individual’s authorization for “health care operations.” Most state statutes do not authorize such a

general use. Indeed, often they are silent as to *uses* of health information. Rather, they list certain *disclosures*, each of which must be compared to see if it fits within the category of “health care operations” as defined in the HIPAA Privacy Rule. This can become a frustrating exercise in comparing apples to oranges.

*Complexity of Analysis Depends on Covered Entity’s Activities and State In Which It Is Located*

The complexity of a preemption analysis is dependent on the covered entity’s practice and the state(s) in which it is located. With the exception of psychotherapy notes, the HIPAA Privacy Rule treats all protected health information the same. In contrast, every state has some statutory provisions that give special treatment to health information related to what may be perceived as “sensitive” medical conditions, such as sexually transmitted diseases and mental health conditions. In some instances, the state laws may impose severe restrictions on the use and disclosure of the information. In others, the state laws may actually permit disclosures that would be prohibited by the general state health privacy statute. Where a covered entity receives or creates information related to these “sensitive” medical conditions, it will have to compare not only the state’s general privacy requirements but also these specific provisions to the HIPAA Privacy Rule.

It should not be presumed that the state law governing information related to a sensitive medical condition is always more stringent than the HIPAA Privacy Rule. For instance, a patient’s right of access to his mental health information is one area where the federal rule may preempt state standards.

Preemption analysis in this area is further complicated by the fact that some sensitive conditions are also covered by public health rules, which are subject to separate preemption standards under HIPAA. In short, providers whose practice area includes these “sensitive” medical conditions will need to undertake an additional level of preemption analysis.

The complexity of preemption analysis also depends on the state in which a provider is located. Some states, such as Pennsylvania and Kansas, have few statutory provisions governing patient access to and the use and disclosure of protected health information by providers. Preemption analysis in these states will be fairly limited (with the exception of regulations and statutes governing specific medical conditions). For the most part, the HIPAA Privacy Rule will establish the privacy standards in these states.

In contrast, the preemption analysis in states, such as California, Wisconsin and Minnesota, that already have comprehensive health privacy statutes will be a complex and time-consuming undertaking. The detailed provisions of these state statutes and regulations must be compared with the equally (if not more) detailed provisions of the HIPAA Privacy Rule. Ironically, this may result in preemption analysis being the most costly in states that already have statutes providing the highest degree of protection for health information.

Of course, if a provider practices in more than one state, the preemption analysis becomes even more complicated. This situation is not unusual even for providers in small practices in jurisdictions like the Washington, D.C., metropolitan area.

*Expected Extent of Preemption of State Laws*

A provision of state law is only preempted to the extent that it is contrary to the HIPAA Privacy Rule. Following well developed case law, the HIPAA Privacy Rule defines a state law as being contrary to the federal law when it is either impossible for the covered entity to comply with both laws or where the provision of state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of the HIPAA Privacy Rule. With respect to uses and disclosures, the HIPAA Privacy Rule is largely permissive. It requires disclosures only to the patient and to HHS for oversight of the federal regulation. In all other circumstances, the rule permits, but does not require, uses and disclosures that meet certain criteria.

Some have speculated that because of this structure (permissive, not mandatory), the HIPAA Privacy Rule will not preempt state laws extensively. There may be some merit to this argument. However, it does not obviate the need to complete a comprehensive preemption analysis to determine what laws, if any, are preempted.

Moreover, the fact that a provision of state law is not preempted may actually complicate compliance efforts. When a state law is not preempted, it remains in effect alongside with the comparable federal provisions. This remains true even when a state provision is “more stringent” than the HIPAA Privacy Rule. State law *does not* preempt federal law. (This aspect of preemption is often misconstrued. On several occasions we have heard the statement that a more stringent state provision preempts federal law.) The net effect is that a covered entity may have to comply with dual standards that vary slightly under federal and state law.

In some circumstances, a covered entity will be able to comply with both state and federal law by complying with the higher standard. For example, while the HIPAA Privacy Rule gives a provider 30 days to respond to a patient’s request for a copy of his medical records, under California law, a provider has only 15 days to respond to such a request. California law is not contrary to the HIPAA Privacy Rule and will remain in effect. Here, by complying with the state provision, a provider automatically will also comply with the federal standard.

But there are many circumstances where this is not the case. For instance, in New York, when a patient is denied access to his medical records he has the right to have the denial reviewed by an access review committee, an independent body appointed by the health commissioner. In contrast, under the HIPAA Privacy Rule the denial of access is reviewed by a health care professional designated by the covered entity. These provisions do not conflict—it is possible to comply with both, and surely the New York statute does not stand as an obstacle to the HIPAA Privacy Rule’s goal of providing patients access to their own health information. The provisions are just different. In this circumstance, the

slightly different state and federal right to review will co-exist. It should be noted, however, that state authorities have recognized this duplicative requirement and are considering eliminating the stronger state standard in order to simplify compliance.

## **II. ISSUE PREEMPTION: IS IT WORTH THE EFFORT?**

Given the complexity of the preemption issue, it is only natural to question whether the effort is worth it. Many in the health care industry have long advocated for total preemption of state law in the health privacy field. They assert that uniformity across state lines would simplify health care administration. But at what cost would uniformity be achieved?

Full preemption would eliminate over 40 years of state efforts in this area. Many state health privacy statutes have been fine-tuned over time to ensure that they work properly. Others have been altered to reflect changes in the health care system. All reflect consideration of serious issues by state legislators. While some states have few statutory privacy protections, a significant number have strong state statutes that afford patients access to their own health information and restrict the disclosure of that information to others. Many of these protections attach to medical conditions that subject patients to stigma and discrimination. Every single state has some health privacy laws that are more stringent than the standards in the HIPAA Privacy Rule.

Full preemption of state privacy laws by the HIPAA Privacy Rule would eliminate these important protections. While undertaking a preemption analysis may be difficult, the answer is not to eliminate all state law. A federal health privacy law should not effectively lower privacy protections.

Rather, HHS and others in the health community should undertake efforts to ease the transition to a federal-state scheme for regulating the privacy of medical information.

## **III. WHAT PROVIDERS NEED VERSUS WHAT IS AVAILABLE**

By Spring 2003, covered entities are expected to be in compliance with the new HIPAA Privacy Rule. Many state laws, however, will remain in effect. Thus, in order to meet this deadline, covered entities need to know what will be required of them under the combination of state and federal law.

Ultimately, what small providers want and need is a compliance manual. We repeatedly hear from small providers (and others) that they want to comply with the HIPAA Privacy Rule and state law –“Just tell us what we need to do.” They want and need a text-based guide that will tell them the specific actions they need to take in various circumstances in

order to comply with both federal and state privacy laws. They do not have the time or the resources to invest in developing this product.

For the most part, there is a dearth of this type of compliance guide available at all, let alone for free or at a low cost. Some preemption analysis that is available to covered entities is expensive. This is not surprising given the complexity of the process. Attachment B to this testimony lists some of the low cost or free preemption materials available on the Internet.<sup>3</sup> Many of these products do not post samples of their analysis, so it is difficult for a consumer to determine if the content or format is useful.

Some of the analysis available is presented in a matrix format that compares a specific provision of state law to the relevant provision in the HIPAA Privacy Rule and reaches a conclusion such as “state law is not preempted” or “follow HIPAA.” These analyses are primarily geared towards lawyers, who should be familiar with the state statutes at issue. This type of analysis provides a crucial step in analyzing what a provider will need to do to comply with both federal and state law. However, it falls short of meeting providers’ need for a simple text-based compliance guide.

In short, there is not much compliance guidance currently available for providers and what is available is generally difficult to assess without purchasing it.

A natural question to ask is what role, if any, the provider associations are playing in furnishing members with guidance on complying with both state and federal laws. Although there appear to be some exceptions, for the most part the provider associations have not taken the responsibility for furnishing their members with guidance that takes into account the interaction of federal and state law. Provider associations appear to be facing a number of challenges in addressing this issue. While many provider associations appear to recognize that preemption analysis is necessary, they face severe fiscal constraints and do not have the resources on hand to finance such an undertaking. It is difficult for them to ask their members for special support when many of their members do not yet recognize the need for undertaking a preemption analysis. Moreover, obtaining a preemption analysis, while costly, would be just the first step in creating a provider-specific compliance guide. As a consequence, most provider associations have not yet addressed preemption analysis in any detail.

This lack of guidance for providers from any source is disturbing. This is particularly true given the looming compliance deadline.

---

<sup>3</sup> This list is not exhaustive, but only includes resources that were easily obtainable.

#### **IV. RECOMMENDATIONS**

Below are some general recommendations of activities that HHS may undertake to help simplify the preemption analysis process. (To the extent HHS may already be pursuing these activities, it should be commended.)

- Publish guidance or a frequently asked question information sheet specifically addressing preemption issues (e.g., state law does not preempt federal law).
- Continue to respond to questions on interpreting the HIPAA Privacy Rule.
- Work with CMS and other state agencies to determine how HIPAA interacts with these other federal laws and publish guidance on these issues.
- Build coalitions with state-based organizations, such as:
  - National Association of Attorneys General (they have a privacy working group)
  - National Governors Association
  - State Medicaid Agencies (who are undertaking a lot of HIPAA analysis)
  - State-based provider associations
- To the extent money is available, issue grants to state health provider associations to undertake the preemption analysis for their particular group. (Once a general guide is completed for a state, it would be very cost-effective to tailor it to other groups.)

#### **V. CONCLUSION**

Preemption analysis is a complicated, time-consuming process. Sole practitioners and providers in small organizations will need much assistance in determining what they need to do to comply with both the HIPAA Privacy Rule and their state health privacy laws. Currently, these resources are sorely lacking. An intensive effort needs to be undertaken immediately if providers are realistically expected to be in full compliance with both their state health privacy laws and the HIPAA Privacy Rule by April 2003.

Attachment A

THE INTERACTION OF ONE SECTION OF THE HIPAA HEALTH PRIVACY RULE AND THE CALIFORNIA PATIENT ACCESS TO MEDICAL RECORDS ACT

DENYING A PATIENT ACCESS TO HIS OWN HEALTH INFORMATION				
ISSUE	FEDERAL RULE	CALIFORNIA STATUTE	INTERACTION	RATIONALE
<b>Type of health information to which access can be denied</b>	Access can be denied to <i>any protected health information</i>	Access can only be denied to <i>mental health records</i>	Access can only be denied to <i>mental health records</i>	Denial of access is permitted under both state and federal law, but CA law allows denial in narrower circumstances. To comply with both, follow CA law.
<b>Who makes determination</b>	where a <i>licensed health care professional</i>	if the <i>health care provider</i>	where a <i>licensed health care professional</i> .	To extent CA law would allow a health care facility administrator who is not a provider to deny access, CA law would be preempted
<b>Standard of risk</b>	has determined in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the <i>individual or another person</i>	determines there is a substantial risk of significant adverse or detrimental consequences to the <i>patient</i> .	has determined in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the <i>patient</i>	Standards are fairly similar. To extent CA. law would permit denial of access where fed. standard would not, CA law would be preempted.
<b>Who is endangered</b>	45 C.F.R. 164.524(a)(3)	Cal. Health & Safety Code § 123115(b) “Mental health records” are patient records that relate to the evaluation or treatment of a mental disorder. “Health care provider” includes specified professionals (such as psychologists) and health care facilities, (such as clinics and hospitals). Cal. Health & Safety Code § 123105.		Denial of access is permissive under both fed. regs. and CA statute, but CA allows denial only if patient is endangered. To comply with both, comply with CA law.

## **Attachment B**

### **SELECTED PREEMPTION ANALYSES FOR PROVIDERS SPONSORED BY PROFESSIONAL ORGANIZATIONS OR THE STATE**

#### Arizona

Arizona Hospital and Healthcare Association  
\$100 for members/\$200 for nonmembers  
No sample analysis available on web site.

#### California

California Office Of HIPAA Implementation (CalOHI)

Charged with statewide leadership, coordination, direction, and oversight responsibilities for determining which provisions of state law concerning personal medical information are preempted by HIPAA.

California Healthcare Association

\$175 for members/\$375 for nonmembers

Analyzes Confidentiality of Medical Information Act & Patient Access to Medical Records Act  
Text based

No sample analysis available on web site

#### Colorado

Colorado Health and Hospital Association

\$1,500 for nonprofits/\$2,500 for forprofits

Statutes, regulations, case law

No sample analysis available on web site.

Preview available at association during business hours

#### Florida

Florida Hospital Association

\$175 for members/\$395 for nonmembers

No sample analysis available on web site.

#### Illinois

Analysis currently being prepared under direction of Governor's office

To be posted on web site of Ill. Department of Public Aid

#### Iowa

Iowa Medical Society, Iowa Attorney General's Office and volunteer group of attorneys preparing analysis to be reviewed by stakeholder groups

Will be available through HIPAA Snip web site

## **Attachment B**

### **SELECTED PREEMPTION ANALYSES FOR PROVIDERS SPONSORED BY PROFESSIONAL ORGANIZATIONS OR THE STATE**

#### Massachusetts

Boston Bar Association.

Available to anyone for \$400 --Bar association members receive further discount

Sample analysis available online

#### Nebraska

Nebraska Hospital Association

Members only

#### New Jersey

New Jersey Hospital Association: Preemption analysis in process

Price not posted

To be made available to NJHA members at a discount

#### New York

Greater New York Hospital Association

\$ - not listed

Analysis limited to institutional health care providers

#### North Carolina

North Carolina Healthcare Information and Communications Alliance

Free

Matrix format

#### Ohio

DRAFT -Ohio State Medical Association & Ohio State Bar Ass'n Health Law Committee

Posted for free- comments solicited

Matrix format

#### Texas

Texas Ophthalmological Association

\$85 for members/\$115 for nonmembers

No sample analysis posted on web.