



GEORGETOWN UNIVERSITY

Health Policy Institute

Testimony before the

**United States House of Representatives
Committee on Ways and Means
Subcommittee on Health**

on

**Health Care Information Technology:
Harmonizing Laws Governing the Confidentiality of
Health Care Information**

**Joy L. Pritts, J.D.
Assistant Research Professor**

July 27, 2005

I. INTRODUCTION

Madam Chairman and Members of the Subcommittee on Health of the House

Committee on Ways and Means: Thank you for the opportunity to testify before you today on protecting the confidentiality of health information and health information technology (IT).

My name is Joy Pritts. I am a lawyer and an Assistant Research Professor at Georgetown University's Health Policy Institute. In my position at Georgetown, I conduct research and analysis on a range of health privacy issues. Much of my work has focused on the Privacy Rule issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), its scope and its interaction with state health privacy laws. I have written extensively on this topic including: *The State of Health Privacy* (2002); *Implementing the Federal Health Privacy Rule in California* (2002); "Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule," *Yale Journal of Health Policy, Law, and Ethics* (Spring 2002); and "Preemption Analysis Under HIPAA—Proceed with Caution," *In Confidence* (April 2003); and state-specific consumer guides on how to obtain and correct or amend medical records under a combination of the HIPAA Privacy Rule and state law, available at <http://hpi.georgetown.edu/privacy/records.html>.

My testimony today will focus on what, if any, actions the federal government should take with respect to protecting the confidentiality of health information in order to facilitate the electronic exchange of health information, including the development of a national health information infrastructure (NHII). In particular, my testimony will address why, at a minimum, the HIPAA Privacy Rule must be expanded to directly cover all who have access to individually identifiable health information. I will also discuss the importance of protecting the ability of states to build on the floor of federal privacy protections, as is currently permitted by HIPAA.

II. BACKGROUND

The electronic exchange of health information has the potential to improve the quality of health care. Electronic records will be more complete, legible, and more accessible to providers. These features should lead to improved quality of care, the elimination of repetitive tests and a streamlining of the administrative process. Under the right circumstances, electronic medical records should also be more secure than paper records.

The risks of a computer-based health information system, however, remain real. Computerization of medical records will make large amounts of detailed personal data more

readily accessible and transferable not only to health care providers but to others. When a breach in confidentiality occurs, it is often with respect to hundreds if not thousands of records at a time. For example, several thousand patient records at the University of Michigan Medical Center containing names, job status, treatment information and other data were inadvertently posted on public Internet sites for two months.¹

Unintentional disclosure is not the only threat to health information in electronic format. Some people improperly access and disclose medical records because they want to make money. A hospital employee sold country singer Tammy Wynette's medical records to the National Enquirer and Star tabloids.² Hospital employees in New York sold emergency room patients' information to attorneys and others to use in insurance scams.³ Recently, an employee of cancer clinic accessed the medical records of a patient with terminal cancer, obtained credit cards in the patient's name, and ran up over \$9000 in charges.⁴

Others improperly access medical information to use against or embarrass a person. As New York Congresswoman Nydia Velasquez testified before the Senate Judiciary Committee, her medical records – including details of a bout with depression– were faxed from a New York hospital to a local newspaper and television station on the eve of her 1992 primary.⁵ On a more local level, the medical records of a Maryland school board member, who had been treated for depression, were sent to school officials as part of a campaign criticizing his performance.⁶

Still others improperly access and disclose medical information out of curiosity. An employee at a major hospital in Washington DC learned that one of her co-workers had HIV when she improperly accessed his medical record to find out why he was hospitalized. The employee revealed the patient's HIV status to other co-workers who ostracized him.⁷ When former President Clinton was in the hospital for heart surgery 17 hospital workers who had nothing to do with his health care improperly tried to access his medical records. Perhaps most

¹ "Black Eye at the Medical Center," *The Washington Post*, February 22, 1999, p. F5.

² Selling Singer's Files Gets Man Six Months," *Houston Chronicle*, December 2, 2000, p. A2.

³ Office of the District Attorney, Nassau County, New York, Press Release, November 23, 2004, available at <http://www.nassauda.org/dawebpage/pressreleases/NUMC%20arrests.htm>

⁴ U.S. Attorney's Office, Western District of Washington, Press Release, "Seattle Man Pleads Guilty in First Ever Conviction for HIPAA Privacy Rules," August 19, 2004, available at http://www.usdoj.gov/usao/waw/press_room/2004/aug/gibson.htm

⁵ A. Rubin, "Records No Longer for Doctors' Eye Only," *Los Angeles Times*, September 1, 1998, p. A1

⁶ C. Samuels, "Allen Makes Diagnosis of Depression Public; Medical Records Mailed Anonymously," *The Washington Post*, August 26, 2000, p. V1.

⁷ P. Slevin, "Man Wins Suit Over Disclosure of HIV Status," *The Washington Post*, December 30, 1999, p. B4.

disturbing was the reaction of the hospital employees, one of whom commented, “I’m not surprised. People are nosy. It happens all the time.”⁸

The risks of having medical information improperly accessed and disclosed are shared by nearly everyone: people going through a divorce or custody dispute; people who work in the health care system and who also happen to be patients of that system; people who live in small communities; and people with medical conditions that may subject them to stigma or discrimination. The consequences can be severe. People fear that they will be ostracized, that they may lose their custody battle, a political race, their job, or their insurance.

As we continue to move toward the computerization of medical information, it is imperative to ask whether there are adequate privacy laws in place to reduce, if not eliminate, these risks. The HIPAA Privacy Rule is not sufficient. It is not broad enough to cover all of those who have access to health information, especially the growing number who will have electronic access. Furthermore, because HIPAA is designed to provide a minimal floor of privacy protections it is important that states retain their ability to offer higher levels of privacy protection.

III. FEDERAL PRIVACY PROTECTIONS SHOULD APPLY TO EVERYONE WHO RECEIVES OR CREATES IDENTIFIABLE HEALTH INFORMATION

HIPAA and the Privacy Rule issued under the Act only directly cover a core group of those who hold and maintain health care information (known collectively as “covered entities”): health care providers who transmit health information electronically in connection with certain financial and administrative purposes, health plans and health care clearinghouses. As the Department of Health and Human Services (HHS) noted, “Unfortunately, this leaves many of the people and organizations that receive, use and disclose protected health information outside of the system of [federal] protection.”⁹ First, HIPAA does not cover all health care providers. Only providers who transmit health information electronically for certain administrative and financial transactions (largely related to insurance) are covered by HIPAA. For example, an increasing number of health care providers offer health services directly to consumers over the Internet, accepting only credit card payments. These providers are beyond the scope of HIPAA.

⁸ J. Lite, D. Epstein and C. Katz, Clinton File Snoopers Rapped,” New York Daily News, September 11, 2004, available at <http://www.nydailynews.com/news/local/story/230961p-198366c.html>

⁹ U.S. Department of Health and Human Services, *Preamble, Standards for Privacy of Individually Identifiable Health Information; Proposed Rule*, 64 Fed. Reg. 59918, November 3, 1999, p. 59923.

Other examples of persons who receive and use information and who are not covered by HIPAA include workers compensation carriers, researchers, life insurance issuers, employers and marketing firms. HHS also lacks the authority to directly regulate many of the persons that covered entities hire to perform administrative, legal, accounting, and similar services on their behalf, and who would obtain health information in order to perform their duties (called “business associates”).¹⁰

Although HHS attempted to fill some of these gaps by requiring covered health care providers and health plans to enter into contracts that require those who perform services on their behalf (known as “business associates”) to protect the confidentiality of the health information that they receive, HHS has no enforcement authority over these recipients. If business associates violate their contracts, HHS cannot impose civil or criminal penalties against them.

Similarly, it appears that HHS may not have the authority to impose criminal penalties against individuals who improperly obtain or disclose individually identifiable health information even if they act for profit. HIPAA provides for criminal penalties for persons who knowingly in violation of the Act obtain or disclose individually identifiable health information relating to an individual.¹¹ The Act provides the most substantial criminal penalties for those who commit these acts under false pretenses or with intent to sell or use the information for commercial purposes, personal gain or malicious harm.¹² The United States Department of Justice has recently taken the position that these criminal penalties generally apply only to covered entities. Employees and others who improperly obtain and use health information (even if it is for profit or to cause serious harm to another) may not be prosecuted under this section.¹³ Under this interpretation, the hospital employees described above who sold emergency room patient information to lawyers could not be prosecuted under HIPAA.

These gaps in federal privacy protection coverage leave large volumes of identifiable health information vulnerable to improper access and disclosure without any real remedies. The promotion of the electronic exchange of health information heightens the urgency of filling these gaps through federal legislation. Forming a national health information infrastructure without

¹⁰ See 64 Fed. Reg. 59923.

¹¹ 42 U.S.C. § 1320(d)-6(a).

¹² 42 U.S.C. § 1320(d)-6(b).

¹³ U.S. Department of Justice, letter for Alex M. Azar II, General Counsel, Department of Health and Human Services, June 1, 2005, *available at* http://www.usdoj.gov/olc/hipaa_final.htm

adequate federal privacy protections threatens not only the privacy of patients but also the very viability of such a system.

III. HIGHER STATE HEALTH PRIVACY PROTECTIONS SHOULD REMAIN IN PLACE

It is important to preserve the ability of states to impose more protective privacy standards on the use and disclosure of health information as we encourage the electronic exchange of health information. As currently written, HIPAA sets a federal floor for the protection of health information. The HIPAA Privacy Rule overrides (preempts) state laws that are less protective of privacy. However, state laws that provide health information privacy protections that are equal to or greater than those contained in the HIPAA Privacy Rule remain in place. These state laws offer additional privacy protection to people with medical conditions that often subject them to stigma or discrimination, such as HIV or mental health conditions. They give patients greater access rights to their own health information.

Many in the health care industry would like to preempt all state health privacy protections so that the HIPAA Privacy Rule would serve as the uniform, national standard for protecting the privacy of health information. However, doing so would directly contradict a key, underlying premise of the HIPAA Privacy Rule. The Rule was explicitly conceived, written and issued as the minimally acceptable standard upon which states could build. Indeed, the ramifications of nullifying stronger state privacy laws are enormous and could be quite negative for patients on a number of fronts.

In considering these issues, it is imperative to remember how we got to where we are today. States have traditionally exercised power over the health and welfare of their citizens. Over the years, states have developed an extensive range of statutes and regulations that protect the privacy of health information. Every state has some statute or regulation governing the use of health information. These laws can be found in health provider licensing laws, insurance laws, public health laws, the rules of evidence and civil procedures. Many states developed statutes and regulations that specifically address the use and disclosure of health information in a detailed and comprehensive fashion. In response to the needs of their citizens, most states have laws that provide privacy protections specifically for information related to medical conditions that are often associated with stigma or discrimination, such as HIV or mental health conditions.

Additionally, in the 40 years preceding the issuance of the Privacy Rule, most states developed common law through court cases where people sued for the improper disclosure of their health information, often based on invasion of the right to privacy. The level of privacy protection afforded by the states, however, varied widely. Some states had broad, detailed privacy protections for health information while others had few protections.¹⁴

As efforts to encourage the health care industry to adopt computer technology intensified it became apparent that there was a need for at least minimum federal standards to protect the privacy of health information. Beginning as early as 1980, Congress attempted to pass health privacy legislation. In 1996, Congress once again took up the issue of health privacy, this time within the context of HIPAA. The Administrative Simplification provisions of HIPAA were designed to encourage the development of an electronically based health care system. Recognizing that protecting the privacy of health information was an important component of this system, Congress set itself a 3-year deadline for enacting comprehensive health privacy legislation. If Congress failed to act in that time, HHS was directed to write and issue health privacy regulations. HIPAA expressly provides that these federal regulations will not supercede a contrary provision of state law if the state standard is more stringent than the standards imposed by the federal regulations.

Congress was unable to pass comprehensive health privacy legislation within the 3-year period. No national consensus could be reached on some of the more difficult policy issues surrounding the protection of health information (such as the appropriate level of protection for HIV information or for genetic information and the right of an individual to sue for improper disclosures of information). Accordingly, the duty to craft federal health privacy protections passed to HHS.

Throughout the rule-making process, HHS consistently maintained that it was establishing minimum federal standards, which would not disturb more protective state laws. In explaining its approach to the Privacy Rule, HHS stated:

It is important to understand this regulation as a new federal floor of privacy protections that does not disturb more protective rules or practices. Nor do we intend this regulation to describe a set of a ``best practices." Rather, this regulation describes a set of basic consumer protections and a series of

¹⁴ See J. Pritts, "Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule," *Yale Journal of Health Policy, Law, and Ethics* (Spring 2002).

regulatory permissions for use and disclosure of health information. The protections are a mandatory floor, which other governments and any covered entity may exceed.¹⁵

In response to public comments requesting additional privacy protection for HIV/AIDS information, HHS again explained that it was taking a minimalist approach:

Where, as in this case, most states have acted and there is no predominant rule that emerges from the state experience with this issue, we have decided to let state law predominate. The final rule only provides a floor of protection for health information and does not preempt state laws that provide greater protection than the rule. Where states have decided to treat certain information as more sensitive than other information, we do not preempt those laws.¹⁶

One and half years later, HHS responded to consumer concerns about the elimination of the requirement that covered entities obtain patient's consent to use or disclose identifiable health information for treatment, payment, and health care operations, by reassuring them that state privacy protections would remain in place. HHS stated:

The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force. In order to not interfere with such laws and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a "best practice" standard.¹⁷

In short, from beginning to end the Privacy Rule has been built on the understanding that it would serve as a minimal floor of protection and that state laws affording higher protections would be preserved.

As a result, many state laws remain in effect. Some of these state laws afford a higher degree of protection to sensitive medical information, such as information related to genetic testing, HIV or mental health. States continue to afford their citizens the right to sue for improper disclosures of their privacy or to obtain their medical records.

Many in the health care industry would eliminate these higher state health privacy protections in the interest of having more uniformity. The Privacy Rule has set minimal

¹⁵ Preamble, Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82461, December 28, 2000, p. 82471.

¹⁶ Preamble, Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. at 82731.

¹⁷ Preamble, Standards for Privacy of Individually Identifiable Health Information; Final Rule (as Modified) 67 Fed. Reg.53192, August 14, 2002, p.53212.

standards in every state. It has effectively created privacy standards in states where few existed and raised standards in those with few protections. By establishing a federal floor of health privacy protections, HIPAA has already substantially evened the playing field. (See App. Fig. 2). Moreover, in response to the HIPAA Privacy Rule, many states have taken the initiative to re-examine their own health privacy laws. As a result, some states have amended their privacy laws, where appropriate, so that they are more closely aligned with the HIPAA standards. In practice, this voluntary action has also produced more uniformity.

Preempting all state health privacy protections in the interest of producing yet more uniformity would have serious and wide spread ramifications. As discussed above, the HPAA standards are meant to be minimum standards. They were never intended to serve as the sole standard for protecting identifiable health information. Eliminating state law and relying on the HIPAA Privacy Rule would effectively lower the privacy protections in place for some of the most vulnerable health care consumers (such as mental health patients and those with HIV). (See App. Fig. 3) In many states, it would overturn hard-fought compromises over some of the very issues on which Congress has not been able to reach consensus. Such an approach would eradicate over 40 years of state common law giving consumers the right to sue for the improper disclosure of medical records. Given the variety of state laws that are designed to protect the privacy of health information it is difficult to predict the full range of consequences of such an approach. It is clear, however, that preempting state health privacy protections would seriously undermine states' traditional ability to protect the health and welfare of their citizens.

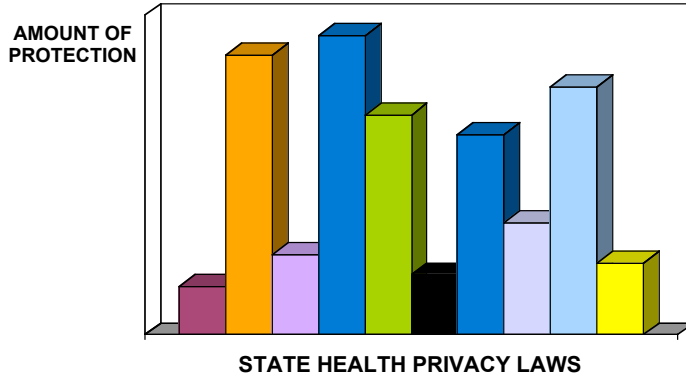
IV. CONCLUSION

As we continue to move toward the electronic exchange of health information and the creation of a national health information infrastructure it is crucial that the privacy of health information not be compromised in the interest of expediency. Federal privacy protections for health information should be expanded to ensure that standards for using and disclosing health information are in place for everyone who receives or creates identifiable health information. Federal law also should ensure that those who improperly obtain use and disclose health information are subject to civil and criminal penalties.

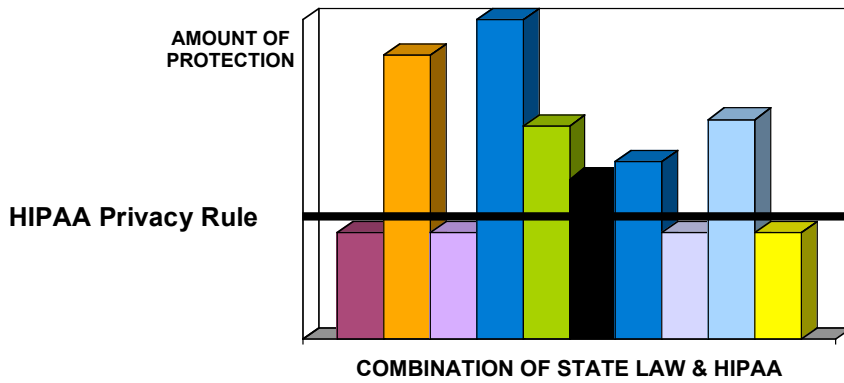
State laws that set higher standards for protecting the privacy of health information should remain in place. The HIPAA Privacy Rule is simply not adequate.

UNIFORMITY—AT WHAT COST?

Health Privacy Protections Before HIPAA (Fig. 1)



Health Privacy Protections After HIPAA (Fig. 2)



Health Privacy Protections -- State Law Preempted by HIPAA (Fig. 3)

