**STATEMENT OF PROFESSOR PETER P. SWIRE**
**C. WILLIAM O'NEILL PROFESSOR OF LAW**
**MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY**
**SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS**

**BEFORE**

**THE U.S. HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES**

**ON**

# THE PRIVACY AND SECURITY OF ELECTRONIC HEALTH RECORDS

**JUNE 19, 2007**

Mr. Chairman, Mr. Ranking Member, members of the Committee:

Thank you for your invitation to testify today on the privacy and security of electronic health records. Our medical system is now striving to move toward what is often called the National Health Information Network. Today, less than 10 percent of our clinical records are accessible in electronic form. All of us hope that that number climbs sharply in the next decade. As my colleague Karen Davenport has stressed in a new report, improved health information technology is essential to improving the quality of our nation's health care.[1]

To make the shift to the NHIN, we need to get privacy and security right. Public surveys repeatedly show that privacy and security concerns are top-of-mind when it comes to the shift to electronic health records. Unless Americans are convinced that effective safeguards are in place, then many of the benefits of the NHIN may be delayed or lost entirely.

My testimony today highlights two key issues—preemption and enforcement.

**First, preemption of state laws would effectively repeal many existing privacy and security protections.** There is a national baseline of protection under the Health Insurance Portability and Accountability Act of 1996. The HIPAA privacy and security rules, on which I worked extensively, offer essential safeguards for patient records. They are incomplete, however. It is the states that provide the current protections for sensitive records such as mental health, HIV, genetic information, and other key categories of records. The NHIN should be an occasion for strengthening safeguards, and not repealing numerous safeguards in the name of federal preemption.

**Second, the current "no-enforcement" system is not a credible basis for EHRs and the NHIN.** HHS has received over 27,000 HIPAA privacy complaints but has yet to bring its first case for civil monetary penalties. HHS has needlessly adopted a "one free violation" policy, guaranteeing covered entities that they can violate the law the first time without financial punishment. And the Department of Justice has interpreted the HIPAA criminal provisions in misguided and narrow ways. As explained below, each of these problems can and should be fixed through targeted legislation or regulatory change.

## Background

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and a Senior Fellow at the Center for American Progress. I live in the Washington, D.C. area.

From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. My biggest single project in that role was acting as the White House coordinator for the HIPAA medical privacy rule. Working with HHS, we announced the

[1] Karen Davenport, "Navigating American Health Care: How Information Technology Can Foster Health Care Improvement," Center for American Progress, May, 2007, *available at* http://www.americanprogress.org/issues/2007/06/health_IT_report.html.

proposed rule in October 1999. There were over 52,000 public comments on the proposed rule. The final rule, including responses to all of those comments, was released in December 2000. Shortly thereafter, I returned to my law teaching position. In 2002, HHS announced modifications to the medical privacy rule. The rule went into full effect in April, 2003.

Since leaving government at the beginning of 2001, I have worked extensively on medical privacy and security issues. My CV details my writings and speeches on these issues. From 2004 until 2006 I was a member of the Markle Foundation's Connecting for Health Task Force. Connecting for Health's Common Framework is an outstanding set of materials about how to create private and secure health information exchange. For detailed discussion of security and privacy issues, I commend those papers to the committee's attention.

Since 2001, in compliance with my university's limits on outside consulting, I have also worked on medical privacy and security issues for private-sector clients, as a consultant to the law firm of Morrison & Foerster, LLP. This work with an array of clients has given me hands-on experience in what it is like to comply with the privacy and security rules. None of these clients has paid me in connection with the testimony today, and the views expressed here are entirely my own.

## Preemption of State Laws Would Effectively Repeal Many Existing Privacy and Security Protections

My first theme today is that simple preemption of state laws would effectively repeal many existing privacy and security protections.

To understand the preemption issue, it is useful to start with the case in favor of preemption made by in industry. This view starts with a correct factual premise—the benefits of sharing electronic clinical data are high. As Newt Gingrich has often said, "Paper kills." We need to move to a more networked version of health care. The shift to electronic records has occurred in banking, travel, and most other sectors, and it is inevitable and desirable for it to occur for clinical health records.

On all of this I agree. The next part of the pro-preemption position asserts that we can only have a national health information network if we have a national set of rules. HIPAA forms that national baseline, and so we should harmonize on the HIPAA standard. In short, goes this argument, preemption is essential to a national network—it's a "no-brainer."

Although I sympathize with the system designers who struggle with diverse state laws, the effects on privacy and security from this sort of preemption would be large and negative. To see why, it is important to realize that protections for the most sensitive categories of medical information are set forth in state law, and not in HIPAA. Here are some categories of medical records that are often protected at the state level today:

- HIV and other sexually transmitted diseases
- Mental health (beyond the limited scope of "psychotherapy notes" defined in HIPAA)
- Substance abuse and alcohol

- Reproductive and contraceptive care (where states vary widely in policy)
- Records held by public health and other state agencies
- Genetic records

The key thing to realize is that HIPAA simply does not have provisions for these topics. If there is federal preemption on the HIPAA baseline, then there will be a large drop in privacy protection, especially for the most sensitive records.

A related point is that many reporting regimes have been linked closely with privacy protections. To take one important example, extra-strict protections for HIV records have been a package deal with HIV reporting requirements. The concern is that individuals will decide not to get tested unless they are promised strong confidentiality. If we repeal these confidentiality protections, such as through federal preemption, then we will face the public health risks from the spread of communicable diseases.

In the medium term, the lack of preemption is likely to be more manageable than many in industry have assumed. Electronic health records are being deployed in regional health information organizations, and many of those RHIOs cover only one or a few states. A New York City RHIO, for instance, could manage the vast bulk of its records by complying with the laws of New York, New Jersey, and Connecticut. As we build out from these regional systems, each RHIO can share its expertise about relevant state laws with other RHIOs. The path toward compliance with state law is thus far simpler than it would be if we tried to do a massive and instantaneous shift to a 50-state system.

As a final point on preemption, the state laws that are often seen as "burdens" by industry have another name from the consumer perspective—consumer "protections." In light of the strong privacy and security concerns about the NHIN, there should be no rush to repeal these state privacy and security protections.

**The Current "No-Enforcement" System Is Not a Credible Basis for EHRs and the NHIN**

I have serious concerns about the current enforcement, or lack of enforcement, of HIPAA privacy complaints. This lack of enforcement creates a major obstacle to public acceptance of EHRs and the NHIN—if no enforcement actions are brought under HIPAA, why should the public trust that there will be effective enforcement as far more medical records flow around the NHIN?

Let me emphasize that my criticism here goes to law and policy, and not to the good will or competence of the individuals at HHS who work on enforcement at the Office of Civil Rights. From my time in the government and since, I have been uniformly impressed with the quality of people who have worked on privacy and security issues.

There are three principal problems:

- First, the batting average at OCR is low, to say the least—zero civil penalties for over 27,000 complaints. Through the end of April 2007, OCR reported a total of 27,070

HIPAA privacy complaints, with over 4,500 resolved through investigation or enforcement. Despite this heavy volume, not a single case has yet resulted in civil monetary penalties.

- Second, the current administration has adopted the policy of "one free violation." In the 2006 enforcement rule adopted by HHS, the decision was made that a covered entity would simply not be subject to civil penalty for its first violation.[2] Instead, the first offense always results in a plan to correct actions going forward. This "one free violation" policy sends the signal that medical privacy rules are not taken seriously—a covered entity can be lax in its protection of patient records, secure in the knowledge that it can fix the problems if and when a complaint is filed.

- Third, the Department of Justice has dropped the ball on criminal prosecution. In a 2005 legal opinion that I have criticized previously,[3] the Office of Legal Counsel interpreted the HIPAA criminal provision extremely narrowly. Under this opinion, even the purchase and sale of hospital records, for criminal gain, could not be prosecuted under HIPAA. Although some of those problems have since been solved,[4] main Justice has failed to bring a single indictment on any of the 393 cases that HHS has referred for prosecution. These are the most serious cases that HHS has found, but none of them has yet resulted in criminal indictment or civil monetary penalties.[5] The lack of Justice Department action on these referrals is important, because the Office of Legal Counsel has stated that no civil monetary penalties may be imposed for actions that are punishable under the HIPAA criminal statute.[6]

This lack of enforcement has been the subject of major stories in *The Wall Street Journal* and *The Washington Post*,[7] but HHS and Congress have not responded to date. As *The Washington Post* quoted one medical records specialist, "They are saying, 'HHS really isn't doing anything, so why should I worry?'"

---

[2]Under Section 160.312, the regulation states that "the Secretary *will* [not may] attempt to reach a resolution of the matter satisfactory to the Secretary by informal means." 71 Fed. Reg. 8390, 8425 (Feb. 16, 2006). Under the regulation, civil monetary penalties can be assessed only if no agreement is reached by informal means. I do not believe that this position is required by statute. Whether or not it is currently required by statute, the Congress could decide to change this policy by new legislation.

[3] Peter Swire, "Justice Department Opinion Undermines Medical Privacy," Center for American Progress (2005), *available at* http://www.americanprogress.org/issues/2005/06/b743281.html.

[4] My understanding is that Department of Justice prosecutors in the field have been able to bring some HIPAA prosecutions under an innovative approach described by Assistant U.S. Attorney Peter Winn, "Who is Subject to Criminal Prosecution Under HIPAA?" *Available at* http://www.abanet.org/health/01_interest_groups/01_media/WinnABA_2005-11.pdf.

[5] I understand that five criminal cases have been brought to date by U.S. attorneys acting on evidence uncovered in their districts, and not based on referrals by HHS.

[6] The Office of Legal Counsel opinion, at note 13, quotes 42 U.S.C. § 1320d-5(b)(1) for this conclusion, and reaches the remarkable conclusion that "the Secretary may not impose civil sanctions for the commission of an act that subjects a person to the possibility of criminal prosecution, regardless of whether the person is in fact punished criminally." This position is peculiar, to say the least. It seems to mean that a covered entity would be better off doing a serious violation that is criminal, in order to avoid any possibility of civil sanctions.

[7] Theo Francis, "Medical Dilemma: Spread of Records Stirs Patient Fears Of Privacy Erosion,"*The Wall Street Journal*, Dec. 26, 2006; Rob Stein, "Medical Privacy Law Nets No Fines," *The Washington Post*, June 4, 2006.

I have been at conferences where covered entities themselves, including military hospitals, have asked HHS for more enforcement. These unusual complaints—calls for more enforcement by those subject to enforcement—have been based on their experience that it is too difficult to get resources and management attention for data privacy and security now that the zero-enforcement system is known. These complaints are echoed by a report from the American Health Information Management Association, which found in 2006 that HIPAA compliance had actually fallen compared with previous years, due especially to lack of resources and management attention.[8]

The lack of HIPAA enforcement will make it harder to build the next generation of electronic health records. Critics will be on strong ground in saying they can't trust the integrity of the current system, much less have the level of trust needed for the greatly expanded flow of electronic records in the NHIN.

To respond to these problems, targeted legislation could address the following:

- First, end the "one free violation" part of the enforcement regulation.

- Second, end the current interpretation where HHS stops its own enforcement efforts in the most serious cases, whenever there is a criminal referral to DOJ.

- Third, overrule the Office of Legal Counsel opinion that incorrectly and unjustifiably narrowed the criminal provisions of HIPAA.

These targeted measures would bring credibility to the HIPAA enforcement system. There was good reason to go easy on covered entities, and help them come into compliance, when HIPAA first took effect. The HIPAA privacy rule was first announced in 1999, though, and it has been in full effect for over four years. Going forward, serious violations should lead to actual penalties. Only in this way will privacy and security practices improve. And only in this way will we have a credible case for the large expansion of electronic records that will come with the NHIN.

## Some Steps May Be Appropriate to Adjust the Scope of Covered Entities

Staff has asked me for comments about the scope of who is considered a "covered entity" under HIPAA. HIPAA primarily applies today to health care providers, health insurers, and health clearinghouses. By contrast, HIPAA does not apply to many health websites or to services where the patients pay only by cash and credit card and there is no health insurance.[9]

The history of the HIPAA statute explains this odd state of affairs. As Congress in 1996 considered the large health legislation that ultimately was enacted as HIPAA, one important goal was to simplify the health payments system and shift payments to electronic form. The

[8] American Health Information Management Association, "The State of HIPAA Privacy and Security Compliance," (2006), *available at* http://www.ahima.org/emerging_issues/2006StateofHIPAACompliance.pdf.

[9] The Pew Foundation and Health Privacy Project address the scope of covered entities in their report "Exposed Online: Why the new federal health privacy regulation doesn't offer much protection to Internet users," (2001), *available at* http://www.pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf

"Administrative Simplification" part of HIPAA thus moved forward, and it applied precisely to those entities that were involved in the electronic payments system—providers, insurers, and clearinghouses (who convert records into standard electronic formats). Late in the legislative process, Congress realized that privacy and security protections should be included as part of the shift to electronic health payments. The scope of these privacy and security protections thus matched the scope of entities included in "Administrative Simplification."

Going forward, it is possible that additional entities should be covered by the HIPAA privacy and security rules. I recommend caution on this topic, however. To take one example, suppose that a person buys a book on breast cancer from an online book store. Should the entire book store be covered by HIPAA because some of the books are on medical topics?

The bookstore example reminds us that the most important regulatory decision is who will be covered by a rule. If Congress broadly increases the scope of "covered entities," then all of HIPAA's privacy and security requirements will apply to a potentially large number of organizations. Any expansion of that sort should be done only after careful study.

There is one area, however, where this committee may appropriately consider new measures. Important categories of government agencies are exempt from HIPAA but permitted by it to gain access to patient records. Under Section 512(b), public health agencies may receive records, and HIPAA does not apply to those agencies once they receive them. Of perhaps even greater concern, there are ways that law enforcement, homeland security, and national security agencies may be gaining access to large numbers of medical records. For instance, HIPAA's national security or public health exceptions might permit these agencies to receive health records to fight "bioterrorism." We know that the Total Information Awareness program led by Admiral Poindexter targeted such medical records. What we don't know is what sort of databases and data mining exist on Americans' health records in the name of national or homeland security. Jim Dempsey of the Center for Democracy and Technology is currently researching this topic. Attention to his forthcoming report and other oversight is warranted on how government agencies are using sensitive medical records.

## Conclusion

This testimony has highlighted reasons to be cautious about preempting state privacy laws. It has suggested targeted measures to make HIPAA enforcement more credible, and has shown areas where oversight is appropriate on the definition of covered entity.

There are other important privacy and security issues that will arise in development of the NHIN. For instance:

- Authentication: how can we identify patients in the NHIN while avoiding creating one enormous database that becomes a risky source of failure?

- Consent: how can patients have an appropriately nuanced right to consent where in the NHIN their records will go, and for which records?

- Audit: as the NHIN links large numbers of organizations, how will audits and other controls enable the organizations to trust that appropriate safeguards are being implemented?

Discussion of each of these issues, and many others, is contained in Connecting for Health's Common Framework. I know of no better resource for understanding how to build privacy and security into the next generation of America's electronic health records.

My thanks to the committee for inviting me to participate today.