



patientprivacyrights

Written Testimony
Deborah C. Peel, MD, Founder & Chair, Patient Privacy Rights

Thank you for the opportunity to testify today on the discussion draft of “Health Information Technology and Privacy Legislation.” I applaud the hard work of this committee and its staff.

My name is Dr. Deborah Peel. I am the founder and chair of Patient Privacy Rights, a national organization that educates consumers about the importance of health privacy, champions smart policies and technologies, and holds industry accountable to protect what’s most valuable—our health, our families and our reputation. We also lead the bipartisan Coalition for Patient Privacy, representing over seven million Americans.

It is fairly well known that I am passionate - to say the least - about privacy. And the reason for that is that I learned about privacy from my patients. As a practicing physician in the field of psychiatry I know that effective treatment depends upon the trust established between a doctor and a patient. When I first entered practice, people came and paid me cash on the barrelhead because they had lost jobs or their reputations were ruined when someone saw their health records that should not have. I have spent thirty years hearing from people whose privacy was violated.

So while I may be passionate, this idea that your most embarrassing conditions should stay private, or that information about YOU should be in your control, is not a radical concept.

In an era when records were kept in manila folders in locked file cabinets, it was not difficult to ensure medical records were private. But we are in a different world today. Today employers, insurers, even law enforcement want access to health records, and with much of this information moving to electronic formats, the risk to patient privacy is very real. **My patients will tell you: existing laws don't go far enough nor do enough.** You'll hear the same from more than 1.3 million Americans this year alone who had their information breached, not to mention another 1,000 of our veterans cared for by Walter Reed Army Medical Center.

Despite the fact that HIPAA requires more stringent privacy-protective state laws and medical ethics to prevail over the privacy 'floor' in HIPAA, the opposite has occurred. HIPAA regulations allowing broad access to personal health information without consent have been widely used as the nation's privacy standard. Data mining and sale of health information is rampant. This was not the intent of Congress.

Privacy in electronic health systems is threatened in three ways:

- 1) Individuals have no control over the use or disclosure of personal health information in electronic systems. That means 4 million providers and their employees decide when, where, and who gets your sensitive data, not you.
- 2) Electronic systems are not secure. A Presidential Cybersecurity Task Force found that attacks on electronic information systems are growing by 20% a year¹, and the Office of Management and Budget found that attacks on federal electronic information systems grew 60% between 2006 and 2007.²
- 3) Health data is extremely valuable. Americans' personal health information is worth billions.

¹ "Cyber Security: A Crisis in Prioritization," President's Information Technology Committee, p. 5 (Feb. 28, 2005)

² "Feds Losing War On Information Security, Senators Told," Govexec.com (March 13, 2008)
http://www.govexec.com/story_page.cfm?articleid=39518&dcn=e_gvet

- Employers and insurers access personal health data to make decisions about employment and coverage.
- In 2006, one prescription data miner reported revenues of \$2 billion dollars.
- In 2006, a national insurer with plans in all 50 states started a business unit that aggregates and sells the data of 79 million enrollees.
- Every prescription in the U.S. is data mined and sold, even if you pay cash.

How do we address these threats? How do we have both progress and privacy?

First, go back to basics. Define privacy. The “P” in HIPAA does not stand for privacy. NCVHS defined health information privacy as “an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.” Without a definition of privacy, we cannot even agree on what needs to be fixed. Here are a few other accepted definitions:

- The *Hippocratic Oath* says “Whatsoever I shall see or hear of the lives of men or women which is not fitting to be spoken, I will keep inviolably secret.”
- The *Code of Fair Information Practices 1974* says “There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.”

They all say the same thing: privacy means control over personal information—if you have no control, you have no privacy.

HHS still has not defined privacy. HHS recently spent \$500,000.00 on a project to develop definitions for electronic health systems. They defined RHIOs, they defined HIEs, they defined lots of things, but they still have not defined privacy.

When privacy is defined, the right to health privacy must be confirmed in statute. Congress must adopt a definition, Congress choose one.

Second, restore Americans’ control over their personal health information. At a minimum, any health IT legislation must codify what Americans assume happens when they visit

their doctors: that what they “say in the doctor’s office stays in the doctor’s office,” and that it is not shared in any way with others without their permission.

Ladies and Gentleman, getting consent, or permission, to disclose your diagnosis of cancer, an STD, a Paxil prescription or even having the flu is not radical. In fact, obtaining consent is easier than ever with health IT. To accept the argument that consent is too burdensome or impractical means we accept that –

~It is O.K. for the health industry to not even *try* to communicate with their customers, the patients, and

~It is O.K. to just let those who have the most to gain and nothing to lose decide how personal information is used.

Well, that is not O.K. What is radical is to destroy the bond of privacy and trust between physicians and patients that has worked for millennia.

In addition to these fundamental additions to the current HITEC draft we ask that you significantly strengthen public participation in this bill. The proposed members of the HIT Policy and Standards Committees are dominated by conflicted appointees from the health industry; their recommendations will reflect their interests. These committees must include sufficient representation by those without ties to government or the private sector, including consumer advocates, privacy experts, scholars, and those with expertise in medical ethics. We offer a number of suggestions in our detailed comments.

Congress must not delegate the power to alter or eliminate Americans’ long-standing rights to health information privacy. Americans clearly want Congress to act to keep their health records private.

- The Markle Foundation Survey found that $\frac{3}{4}$ of the public want the government to set rules to protect the privacy and confidentiality of electronic health information, and

- Two-thirds want the government to set rules controlling the secondary uses of information.
- Federal Computer Week found that 66% of Americans believe Congress should make protecting information systems and networks a higher priority.³

The lack of privacy is both harmful and deadly. Millions of Americans avoid doctors and delay care for fear their employer will find out, their insurer will drop them or a vast world of strangers will know their most intimate details.

- According to HHS, **two million** Americans with mental illness do not seek treatment for this reason.⁴
- **600,000** cancer victims do not seek early diagnosis and treatment.⁵
- **Millions** of young Americans suffering from sexually transmitted diseases do not seek diagnosis and treatment (1 in 4 teen girls are now infected with a STD).⁶
- The California Health Care Foundation found that **1 in 8** Americans have put their health at risk by engaging in privacy-protective behavior: *Avoiding their regular doctor - Asking a doctor to alter a diagnosis- Paying privately for a test - Avoiding tests altogether.*⁷
- The Rand Corporation found that **150,000 soldiers** suffering from Post-Traumatic Stress Disorder (PTSD) do not seek treatment because of privacy concerns.⁸

The lack of privacy contributes to the highest suicide rate among active duty soldiers in nearly 30 years. CBS News reports an average of 18 veterans commit suicide every day. Soldiers

³ Federal Computer Week, May 23, 2006

⁴ 65 Fed. Reg. at 82,779

⁵ 65 Fed. Reg. at 82,777

⁶ 65 Fed. Reg. at 82,778

⁷ CHCH Consumer Health Privacy Survey, June 2005

⁸ "Invisible Wounds of War", The RAND Corp., p. 436 (2008)

know their treatment and records are not private. This is unacceptable statistic for our men and women in uniform.

To build a system people trust, we need a definition of privacy, and we need to restore the right to health privacy. Millions will not agree to treatment without the guarantee their health records will be private.

I've been sitting face to face with patients for over thirty years. It is that human contact that makes me so passionate about privacy. Frankly, it is heart breaking to see the real destruction caused when private, intimate information gets in the wrong hands. Patient Privacy Rights, in operation for just a few years, hears daily from patients from every state in this nation, desperate for help and looking for justice.

We will always have nosy neighbors. We will always have security breaches at some level, regardless of the security standards we implement. The one thing you can do and must do is minimize what happens to our private information on a daily basis.

I am very grateful for your time and this opportunity to come before you. We respectfully submit our written, detailed comments for this draft legislation as well.