HIPAA and Health Privacy: Myths and Facts

Part 2 — January 2009

This paper answers common myths about HIPAA and health privacy. These facts correct long-standing myths about the right to privacy, patient consent and rights, enforcement of HIPAA provisions, Internet-based health services, the interaction between HIPAA and state laws, information disclosures, marketing, and de-identified data.

A great deal of misunderstanding persists about the current federal health privacy law. This confusion is partly responsible for the public's substantial lack of trust in health information systems. It is well documented that patients' concern about the privacy of their health information directly undercuts both access to, and the quality of, care in this country.

The Privacy Rule enacted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) established the first federal, comprehensive protections for health privacy. The HIPAA Privacy Rule was a landmark in privacy protection. At the same time, it is widely recognized that the regulation is insufficient to protect patient privacy in the new and rapidly evolving e-health environment.

The Health Privacy Project at CDT is working for the adoption of a comprehensive privacy and security framework that sets clear parameters for access, use and disclosure of personal health information for all entities handling health information. Such a comprehensive framework should include appropriate modifications to the Privacy Rule for electronic records held or managed by entities within the traditional health care system. It should also include appropriate protections for health information accessed, maintained or managed by entities outside of the health care system. (For more information on the attributes of a comprehensive privacy and security framework, see http://www.cdt.org/healthprivacy/20080514HPframe.pdf.)

We cannot have a meaningful dialogue about how to improve the HIPAA Privacy Rule and build a more comprehensive privacy framework until we have a shared and clear understanding of what protections exist in current law — and where the law falls short. Shortly after the Privacy Rule took effect, the Health Privacy Project issued a "myths and facts" document to correct misunderstandings about the Rule that were widespread at the time (see

http://www.cdt.org/healthprivacy/20080311mythsfacts.pdf). The purpose of Part 2 is to dispel new myths about the law and replace them with facts in order to facilitate productive discussions about how to build on HIPAA to create a comprehensive set of privacy and security protections for electronic health information.

The Right to Privacy, Before and After HIPAA

MYTH: The HIPAA "Privacy Rule" is really a "Disclosure Rule;" HIPAA took away privacy rights that are based in the Constitution and common law.

FACTS:

- Prior to HIPAA, there was no national health privacy law, and there were no federal limits on how health care providers, employers or insurers collected and shared health information, both within and outside of the healthcare system. There was no federal right granting people access to their health information. Patients instead had to depend on state law if and when it applied.
- Although courts have found a federal Constitutional right to privacy in medical information, that right does not apply to uses and disclosures of health information by private entities. Further, courts have never held this right to be absolute and instead typically weigh a patient's interest in medical privacy against the societal interest in promoting the sharing of health information for certain purposes. (See, for example, *Whalen v. Roe*, 429 U.S. 589 (1977), and *U.S. v. Westinghouse Elec. Corp.*, 638 F. 2d 570 (3d Cir. 1980).)
- In many ways, the common law privacy protections for health information – which still apply – are limited. For example, disclosure of protected health information has always been permitted for a range of purposes, including to insurance companies and for national security, public health monitoring, and law enforcement.
- The HIPAA Privacy Rule was the first, and is still the only, comprehensive federal health privacy law. The Privacy Rule permits health care system entities to use and disclose personal health information for routine health care activities (such as treatment, payment, and certain administrative functions – "health care operations"). Although policymakers should re-examine these permitted uses – especially the exception for operations – and clarify or tighten them for the new e-health environment, the Privacy Rule does not sanction widespread use and disclosure of identifiable health information in contravention of patient privacy interests. To the contrary, the Rule:

- Requires health care providers to give individuals notice of their rights and to inform them about how their health information will be used;
- Grants individuals the right to see and copy their own medical records;
- Imposes limits on disclosing patient records to employers;
- Broadens the scope of protection for health information used by privately-funded researchers;
- Imposes some (but not sufficient) limits on marketing uses of health data;
- Puts safeguards in place for disclosure of health records to law enforcement; and
- Authorizes civil and criminal penalties for violations of health privacy (however, application of these penalties has been essentially non-existent, as explained in more detail below).

MYTH: HIPAA eliminated traditional doctor-patient or therapist-patient "privileges" (i.e., confidentiality).

FACTS:

- Common law privileges were not affected in any way by HIPAA. All confidentiality obligations that traditionally applied to doctors, therapists and other health care providers still apply.
- As noted above, HIPAA permits – but does not require – disclosure of health information for certain activities. Providers may choose not to use or disclose medical information, allowing them to comply with any ethics rules or other professional obligations that impose more stringent confidentiality protections than are found in the Privacy Rule.
- The HIPAA Privacy Rule mandates disclosure of health information 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.
- The relevant sections of the Privacy Rule are found at 45 Code of Federal Regulations (CFR) §§ 164.502, 164.508, 164.512, 164.520, http://www.hhs.gov/ocr/privacysummary.pdf (pages 4-11).

Patient Consent and Patient Rights

MYTH: HIPAA eliminated the "right of consent."

FACTS:

- Prior to enactment of HIPAA, there was no federal "right" to consent or to

withhold consent for the use or disclosure of health information. Doctors, other health care providers and insurers used patient data for a range of purposes without notice or consent.

- Before the final Privacy Rule went into effect, an earlier version did require entities to obtain patient consent to use health information for treatment, payment or health care operations – but providers could have refused to treat, and plans could have refused coverage, if consent was withheld. In contrast, the Privacy Rule that took effect permits use and disclosure of information for these purposes without the need to first obtain consent. Further, for those uses and disclosures requiring express patient authorization (e.g., marketing), providers and plans may not condition treatment or coverage on obtaining authorization.
- Further, HIPAA put in place new rules that give people the right to opt-out of hospitals sharing directory information or disclosing information to family and friends. The Privacy Rule also established new rules requiring patient authorization for disclosure of personal health information to employers, researchers, marketers, and others outside the core health delivery and payment arena.
- For more information on the consent provisions in the Privacy Rule, see http://www.hhs.gov/news/press/2002pres/20020809.html.

MYTH: Requiring consent for all uses and disclosures of health information is the best way to protect privacy.

FACTS:

- Consent is one element of privacy, but it is not a panacea. If health privacy rules ignore the full range of privacy and security protections, and instead rely only (or significantly) on consent, the result will be less protective of privacy and confidentiality.
- A consent-based system – without other legally enforceable limits – unfairly shifts the burden for protecting privacy to patients. Unfortunately, patients are often asked to consent at times when they are least able to make complicated decisions about use of their health data.
- Solely relying on consent to protect patient privacy is likely to result in healthcare providers presenting patients with "blanket" consent forms that authorize the release of information to many kinds of entities for many purposes.
- Most people don't read the details of a consent form and are likely to do whatever they perceive to be required to obtain needed care or insurance coverage.

- If consent becomes the main privacy protection, patients will be exposed to unregulated and potentially non-contemplated uses – and misuses – of their data. Further, the healthcare industry, including new participants, such as providers of personal health records (PHRs), would have fewer incentives to design systems with stronger privacy and security protections.
- For more on the appropriate role of consent policy, see http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.

MYTH: Consumers do not have the right to an electronic copy of their health records.

FACTS:

- Under the "right of access," HIPAA gives individuals the right to request copies of their own health information from a covered entity. HIPAA also requires that a covered entity provide information in the requested form or format if it is "readily producible."
- The preamble to the Privacy Rule states, "if the covered entity maintains health information electronically and the individual requests an electronic copy, the covered entity must accommodate the request, if possible."
- However, some record holders resist providing individuals with a copy of their health information in the format requested. Further, the Privacy Rule permits record holders to take up to 30 days (or more) to provide individuals with copies of their records. The law should be amended to make the obligation to provide electronic copies more explicit, and to facilitate the prompt release of this information to patients.

- See 45 CFR § 164.524 45 for further details.

Enforcement

MYTH: HIPAA includes adequate enforcement provisions, which have been vigorously enforced by the Bush Administration.

FACTS:

- The HIPAA statute provides HHS with the authority to investigate complaints for violations of the Privacy Rule and to impose civil monetary penalties, but this authority is not absolute or sufficiently comprehensive. For example, the statute prohibits the imposition of penalties when the violation is corrected by the entity in 30 days, and the HIPAA regulations require the Secretary to try to first informally resolve all HIPAA complaints.

Further, HHS cannot enforce HIPAA against "business associates" – persons or entities that handle health information because they are performing a function or service for a provider or a health plan. The provider or health plan can only be held accountable for the unlawful actions of its business associates only if there is a pattern of activity that rises to the level of a "material breach or violation." (See 45 CFR §160.504(e)(ii).)

- HIPAA regulations provide the federal government with the authority to routinely audit entities covered by HIPAA to determine if they are complying with the HIPAA security rules, but the regulations do not give HHS the authority to routinely audit for compliance with the Privacy Rule.
- In addition, the Privacy Rule does not give individuals the right to sue, even if they are victims of egregious violations. Instead, individuals can only file a written complaint with the Secretary of HHS via the Office for Civil Rights.
- The Bush Administration has not aggressively enforced the HIPAA Privacy Rule. Although the HHS Office of Civil Rights (OCR) has received roughly 30,000 complaints about HIPAA violations, it has not issued a single civil monetary penalty.[1] Weak enforcement significantly undermines HIPAA, making it a right without a remedy.
- The Department of Justice has pursued only a handful of crimination violations of HIPAA and has narrowly interpreted the law's criminal provisions. For example, DOJ's Office of Legal Counsel has concluded that only covered entities can be held criminally liable for privacy violations, which means that individual health care workers who knowingly access or disclose health information in violation of HIPAA cannot be held responsible unless they were acting at the direction of the covered entity (which is unlikely to be true in the case of criminal conduct). Under this interpretation, some of the most egregious violations of the law would go unpunished.
- For more on enforcement of HIPAA, see §§ 160.306, 160.312 (a)(1), and 160.304(b) of the Privacy Rule and the statutory provisions beginning at 42 U.S.C § 1320, http://www.hhs.gov/ocr/hipaa.

[1] In July 2008, HHS announced that Seattle-based Providence Health & Services agreed to pay $100,000 as part of a settlement of multiple violations of the HIPAA regulations (largely the HIPAA security rules). But the press release from HHS made clear that this amount was not imposed as a civil monetary penalty.
(http://www.hhs.gov/news/press/2008pres/07/20080717a.html)

New Internet-Based Health Services

MYTH: Current law adequately protects health information on the Internet.

FACTS:

- HIPAA directly applies only to certain "covered entities" – health care providers, health plans, and healthcare clearinghouses. There is no general federal privacy law that protects personal information in other contexts.
- Many entities and organizations that collect, store or use health records via the Internet, such as providers of on-line Personal Health Records (PHRs), or that exchange information electronically, such as Health Information Exchanges (HIEs) or Regional Health Information Organizations (RHIOs), are not covered by HIPAA or any other specific federal privacy law.
- Whether a particular PHR is covered by HIPAA depends on whether the provider of the PHR is a HIPAA-covered entity itself or has signed a business associate agreement with a covered entity. Many are neither, so HIPAA does not apply to them. Only those RHIOs and HIEs that have voluntarily signed business associate agreements with covered entities are required to comply with HIPAA rules (and in such a case, they are only contractually obligated to do so). As noted above, business associates are not directly regulated under HIPAA
- Under its unfair and deceptive trade practices authority, the Federal Trade Commission (FTC) can require a private, for-profit entity to comply with whatever the entity states in its published privacy policy. However, the FTC has limited authority to control what an entity promises in its privacy policy and cannot require that an entity have a privacy policy in the first place.
- Some have suggested that the federal Electronic Communications Privacy Act (ECPA) protects health information stored in PHRs. However, coverage under ECPA depends on how the PHR is structured. For example, ECPA will not apply to PHRs that are not available to the public. Further, ECPA may not apply where the PHR service analyzes a person's health information to deliver health advice or targeted advertising. Moreover, even if ECPA applies, the protections of ECPA can be overridden by individual consent. The limits of consent discussed above apply also to PHRs: When patients initially sign up for a PHR service, the PHR provider may seek and obtain blanket consent to a wide range of uses and disclosures. The adequacy of the consent would turn on how clearly the provider described its practices and how explicit the consent was, but these questions mean that the amount of protection ECPA offers is uncertain.

MYTH: The privacy of Internet-based health information services, such as PHRs, can be protected simply by expanding the definition of "covered entity" under HIPAA.

FACTS:

- The HIPAA Privacy Rule was designed to protect information used by and exchanged among traditional health care entities. As a result, personal health information is permitted to flow under HIPAA without patient authorization for certain purposes related to treatment and payment for care. However, the emerging business environment of online health records is very different from the landscape contemplated by HIPAA.
- While the PHR landscape is still evolving, it appears that some PHRs will be supported in whole or part by advertising revenue and partnerships with third-party suppliers of health-related products and services. As a result, people using these tools will be more likely to be marketed to on the basis of health information in their PHI. They will likely be subjected to the tools that Internet companies typically use to gather information about consumer preferences (such as cookies), so that the companies can target them with specific ads or product offers. The data of those using PHRs may be more likely to be sold to third parties (such as pharmaceutical companies and health insurers). Users also will likely be solicited by the PHR's formal and informal business partners, who will likely urge users to share their data for multiple business purposes.
- Applying the Privacy Rule to PHRs only gives individuals a right to authorize—or limit—certain marketing or commercial activities before they can take place.
- Total reliance on individual authorization or consent places people in an unfair and potentially dangerous situation, shifting the burden of protecting privacy solely to the individual and putting the bulk of the bargaining power on the side of the entity offering the PHR.
- As noted above, consent or authorization alone provides very weak privacy protection, particularly when personal health information is stored or exchanged through commercial entities. For PHRs to flourish, clear rules are needed regarding marketing and commercial uses of information that will better protect consumers by restricting PHR vendors from engaging in certain practices.
- Until such rules are in place, getting companies to follow business "best practices" will help protect consumers. One positive development is the endorsement by a number of the major Internet-based PHR vendors of the Markle Foundation's "Common Framework for Networked Personal Health

Information," http://www.connectingforhealth.org/phti/index.html, which provides detailed recommendations for the protection of personal health information in PHRs and other consumer-facing health IT tools. In addition, the Health Privacy Project, the California Healthcare Foundation and a group of corporate leaders released Best Practices for Employers Offering Personal Health Records (PHRs) in December 2007, which provide helpful guidance to guidelines for employers seeking to offer PHRs to their employees (see http://www.cdt.org/healthprivacy/2007Best_Practices.pdf).

HIPAA and State Laws

MYTH: HIPAA preempts stronger state privacy laws.

FACTS:

- HIPAA explicitly does not preempt more stringent state laws – only those that are weaker and inconsistent. (See Section 1178 of the Social Security Act.)
- The states have an important role to play in the articulation and enforcement of health privacy rights, and many have adopted privacy rules for health information that are stronger than the HIPAA Privacy Rule.

MYTH: State health privacy laws that are stronger than HIPAA are a barrier to the development of health information technology and should be preempted.

FACTS:

- The HIPAA Privacy Rule provides a privacy "floor." This means that state laws can provide a higher degree of privacy protection, and many do, particularly with regard to specific sensitive health conditions.
- State health privacy laws were developed to meet the needs of particular populations; preemption of them would put these populations at risk.
- Preemption of state health privacy laws would cause more confusion because many of those privacy provisions are woven into laws that address other topics, such as HIV testing and public health reporting. Eliminating only the privacy provisions of such laws would compromise their integrity.
- Systems can be designed to comply with the laws of the state disclosing the information regardless of where it is being sent.
- See the 2007 report by George Washington University available through http://www.bna.com, Vol. 15, No. 11, 3/19/2007.

Disclosures of Health Information to Employers

MYTH: HIPAA allows a health plan or doctor to share personal health information with an employer.

FACTS:

- The Privacy Rule prohibits healthcare providers and plans from disclosing personal health information to employers without an individual's explicit, written authorization. A valid authorization under the law must include a description of the information to be shared, the name of the person allowed to use or disclose the information, an expiration date, and the signature of the individual.
- The Privacy Rule covers employers who self-insure (that is, employers who are acting in the capacity of a health plan for their employees). Health information collected by such employers for health plan administration purposes must be used for those purposes only and not for making employment-related decisions. The Privacy Rule requires such employers to construct an organizational "firewall" so that the health information collected for insurance administration purposes cannot be shared elsewhere in the company.
- Some employers do collect health information independently, such as through workforce surveys, pre-employment physicals, or to grant leave under the Family and Medical Leave Act. This information is typically collected with the employee or prospective employee's written authorization, but it is not covered by HIPAA. Employers' collection and use of employee medical data is an area that should be examined to determine if there is the need for expanded privacy rules.
- See 45 CFR §§164.508(a)(1), 164.504(a).

Marketing

MYTH: HIPAA permits the widespread use and sale of personal health information for marketing.

FACTS:

- The HIPAA Privacy Rule prohibits providers, plans, and other covered entities from disclosing identifiable health information to a third party for marketing purposes without written authorization from the patient.
- However, the use or disclosure of medical information is explicitly permitted

for certain health related marketing under the Privacy Rule. 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 healthcare provider is paid to encourage the patient to use the product or service.

- Thus, the use of personal health information for marketing purposes is not as widespread as some purport, but the HIPAA marketing rule does contain significant loopholes. For example, providers and health plans are permitted to use personal health information without authorization to send health-related marketing communications that are paid for by third parties, such as pharmaceutical companies and device manufacturers. The rule should be tightened, and there is a strong need for better enforcement.
- For the marketing provisions of the Privacy Rule, see 45 CFR §§164.508(a)(3), 164.50, http://www.hhs.gov/news/press/2002pres/20020809.html.

De-Identified Data

MYTH: All "de-identified" health information can be easily re-identified.

FACTS:

- The Privacy Rule establishes a specific mandate and process for the de-identification of data. Once health information qualifies as "de-identified," the information is no longer protected under the Privacy Rule.
- Due to the widespread availability of personally identifiable information and advancement in analytic capabilities, de-identified data is easier to re-identify now than it was when the Privacy Rule was implemented, although the extent to which de-identified data is actually re-identified is unknown.
- It is illegal to for covered entities and their business associates to re-identify data, but this may be impossible to enforce. Further, de-identified data can be shared with entities not covered by the Privacy Rule – and the federal government cannot pursue penalties against non-covered entities that re-identify data.
- CDT will be publishing a white paper on de-identification of health information and the HIPAA standard. Congress should hold hearings on the appropriate policies concerning deidentification of data, and the Secretary of HHS should consider whether the HIPAA de-identification standard needs to be updated.