

ROBERT GELLMAN
Privacy and Information Policy Consultant
419 Fifth Street SE
Washington, DC 20003

202-543-7923
Fax: 202-547-8287
rgellman@cais.com

Health Privacy in the United States: New Rules for 2003

By Robert Gellman
Privacy and Information Policy Consultant

Prepared for the
23rd International Conference of Data Protection Commissioners
Paris, France
September 24-26, 2001

Introduction

Health privacy in the United States is a complex subject. Until new federal rules take effect in 2003, the privacy of health records has been primarily regulated through state laws. Most states have dozens of different laws that address some aspect of health privacy.¹ The scope and degree of protection afforded to patient information by state laws vary tremendously, and it is unclear how the laws apply to health records that cross state borders. Some federal laws address health privacy, but their scope has been limited.²

Attempts to pass federal health privacy legislation have a twenty-year history of failure.³ In 1996, Congress enacted the Health Insurance Portability and Accountability Act⁴ (HIPAA). The stated purpose of HIPAA is to improve the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards for the electronic transmission of health information.⁵ One effect of HIPAA will be to increase the flow of electronic health data between providers, insurers, employers, processors, government, and others for such routine functions as enrolling an individual in a health plan; checking insurance eligibility, filing a reimbursement claim for delivered health care, requesting additional information to support a claim, and coordinating claims across different insurance companies.

In passing HIPAA, Congress recognized the importance of privacy in an electronic health environment. However, Congress continued to be unable to agree on the terms of a privacy law. Instead, HIPAA provided that if Congress failed to enact health privacy legislation by 1999, the Secretary of Health and Human Services would be required to issue regulations.⁶ Congress did not meet its deadline, and the administrative process began. It took several years before the Secretary finally promulgated the privacy rules. Pressure from the impending end of the Clinton Administration broke through the last bureaucratic barriers.

The HIPAA regulations⁷ were issued in late December 2000. Compliance with the rules is not required until April 2003, and it is certain that the rules will change before compliance is

¹ See, e.g., Institute for Health Care Research and Policy, The State of Health Privacy: An Uneven Terrain (1999) <http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm>.

² The Privacy Act of 1974, 5 U.S.C. §552a, which established fair information practice rules for personal record held by federal agencies, covers health records that the agencies maintain. Other federal laws (38 U.S.C. §7332; 42 U.S.C. §290dd-2) cover drug and alcohol abuse treatment records maintained by any institution that receives federal funds. Scattered other federal laws may touch on health record confidentiality, but together, all federal laws (other than HIPAA) affect only a fraction of health records and health record keepers.

³ See, e.g., U.S. House of Representatives, Committee on Government Operations, *Federal Privacy of Medical Information Act*, H.R. Rep. No. 96-832, Part I (1980) (report to accompany H.R. 5935); U.S. House of Representatives, Committee on Government Operations, *Health Security Act*, H.R. Rep. No. 103-601, Part 5 (1994) (report to accompany H.R. 3600). Both of these bills were reported out of Committee, but neither was enacted into law.

⁴ Public Law No. 104-191, 110 Stat. 1936 (1996).

⁵ 110 Stat. 2021, §261.

⁶ Public Law No. 104-191, §264(c), 110 Stat. 2033 (1996).

⁷ Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information*, 65 Federal Register 82462-82829 (Dec. 28, 2000) (codified at 45 C.F.R. Parts 160 & 164).

required. In 2001, the Secretary issued interpretative guidance⁸ and promised to fix some problems with the rules that had already been identified. As of late February 2002, revisions to the rules have not yet been proposed, and they may not be finished for six months or more after the initial publication of the draft.

Substantive Rules

The HIPAA privacy rules establish national privacy standards and fair information practices that will provide a basic level of protection. The HIPAA rules are lengthy and complex, and they cannot be summarized easily or quickly. The rules are also controversial. Nearly every provision has been the cause of heated debate. It is only possible to highlight a few of the limitations, protections, and gaps that reveal compliance with or deviation from international fair information practice standards.

1. Limitations. HIPAA does not apply to all health information or to all health record keepers. The law applies directly only to *covered entities*,⁹ which are health care providers, health plans (e.g., insurers, health maintenance organizations), and health care clearinghouses (organizations that facilitate the processing of health care claims and information). No other health care record keepers are covered directly. For example, if an employer, school, law enforcement agency, researcher, court, or other organization maintains health information and the organization is not acting as a covered entity, the HIPAA rules do not apply.

An organization that is not a covered entity may still become subject to the HIPAA rules if it functions as a *business associate* for a covered entity. A business associate is someone who carries out a function involving the use or disclosure of individually identifiable health information on behalf of a covered entity. For example, if a hospital hires an independent organization to manage the hospital's record room, the organization will be a business associate of the hospital. The hospital will be required to ensure that its business associate protects information in accordance with the HIPAA rules.¹⁰ The business associate policy extends protections beyond the immediate domain of covered entities. However, if a hospital discloses patient data to a law enforcement agency, the information may not be protected under the rule. A law enforcement agency is not likely to be either a covered entity or a business associate.

The intersection between HIPAA and state laws on health privacy suggests another limitation. The statute provided that any federal privacy regulations shall not supersede a contrary provision of State law if the provision imposes requirements that are more stringent than the federal regulatory requirements.¹¹ Thus, HIPAA establishes a privacy floor that will provide a minimum degree of protection for all covered health records throughout the United States. State laws with lower standards will be superseded. However, each state law that affords a greater measure of privacy protection will remain in force. Privacy advocates see this as an important protection for patients, who will receive the most protective laws at either the state or federal levels. The health care industry generally sees the failure to preempt all state laws as creating a

⁸ See <<http://aspe.hhs.gov/admsimp/final/pvcguide1.htm>> issued on July 6, 2001.

⁹ 45 C.F.R. §160.103.

¹⁰ 45 C.F.R. §164.502(e).

¹¹ 110 Stat. 2021, §264(b)(2).

complex and hard to implement set of different rules that will be expensive to comply with in an environment where records cross state lines routinely during treatment and payment.

2. Protections. One feature of the HIPAA privacy rules most consistent with international fair information practice standards is the requirement for transparency. Each covered entity must prepare and provide to individuals a notice of privacy practices.¹² The notice must describe how patient information may be used and disclosed. It must also describe an individual's rights and the covered entity's legal duties with respect to patient data. The information required to be included in a HIPAA notice of privacy practices is often unavailable to patients in the United States today.

HIPAA also imposes on each covered entity a series of administrative requirements.¹³ These include: 1) designating a privacy official responsible for development and implementation of privacy policies and procedures; 2) training staff in privacy; 3) establishing appropriate administrative, technical, and physical safeguards to protect the privacy of information; 4) establishing a complaint process for individuals; and 5) developing and maintaining written policies and procedures for implementing the privacy rules. These and other administrative requirements may appear to be elementary, but many health care institutions do not have a formal privacy structure or policy. One consequence of the HIPAA rules may be to change the culture of health records, which today is characterized by widespread sharing of patient data among health care institutions with little attention to privacy concerns. Covered entities will be required to pay attention to how records are used, maintained, and disclosed, and this will be a novel requirement for some.

3. Gaps.

One of the most controversial provisions is the requirement that each patient must consent to uses and disclosures for treatment, payment, and health care operations.¹⁴ The use of the term *consent* is confusing because the rule states that each patient may be required to sign a standard consent form as a condition of receiving treatment or as a condition of having an insurer pay for the treatment.¹⁵ It is likely that every provider and payer will insist that a patient sign the standard consent. Under these conditions, mandatory consent is an oxymoron. The standard consent form will authorize the use and disclosure of patient information for many activities. The term *health care operations* includes quality assessment, outcomes evaluation, underwriting, legal services, auditing, business planning, customer service, and numerous other functions.¹⁶

Part of the controversy is due to the mandatory nature of the consent. The rules seem to address the issue in part by giving each patient the right to request that a covered entity modify the standard terms.¹⁷ However, the covered entity has no corresponding duty to honor or even respond to a patient's request.¹⁸

¹² 45 C.F.R. §164.520.

¹³ 45 C.F.R. §164.530.

¹⁴ 45 C.F.R. §164.506.

¹⁵ 45 C.F.R. §164.506(b).

¹⁶ 45 C.F.R. §164.501.

¹⁷ 45 C.F.R. §164.506(c)(4)(i).

¹⁸ 45 C.F.R. §164.506(c)(4)(ii)

Some object that there is nothing consensual about the consent provision. Patients have no choice at all. Others believe that seeking patient consent is nevertheless important because it serves to educate patients about privacy rights and information flows. The health care industry sees the consent requirement as an expensive paperwork burden. Most industry representatives want to eliminate consent for treatment, payment, and health care operations altogether and to replace it with use and disclosure authority under the rule without any role for the patient. Others would like to broaden even further the disclosures permitted as health care operations.

In addition to the disclosures permitted under the consent form, the rules permit numerous uses and disclosures for which patient consent is not required. Patients need not consent, and cannot object, to uses and disclosures for public health, research, law enforcement, health oversight, abuse reporting, judicial proceedings, emergencies, organ donations, and for other purposes.¹⁹ Many of these categories of authorized uses and disclosures include subcategories. Depending on just how the categories are counted, the rules permit two dozen or more nonconsensual uses and disclosures. In many of these instances, when information is disclosed, it escapes the HIPAA regulatory scheme altogether.

Many of the nonconsensual uses and disclosures include specific requirements and procedures that must be met before a record can actually be transferred for the specified purpose. These rules and procedures are also controversial. For example, disclosure to law enforcement is permitted in response to an oral request, without any requirement for review of the request by a court, supervisory official, or independent authority.²⁰

Another part of the rules allows a covered entity to use and disclose patient data for marketing and fundraising activities.²¹ The marketing provision has been especially controversial. A covered entity that reserves the right to use records for marketing through its notice of privacy practices can use or disclose the records without advance patient consent and without even giving a patient the right to object in advance. Patients only acquire the right to object to marketing uses after they have received a marketing communication. The marketing rule is particularly complex, riddled with loopholes, and appears directly inconsistent with prevailing medical ethics. It is so broad that information about psychiatric treatment, sexually transmitted diseases, or other sensitive ailments can be disclosed to marketers at times. Virtually every covered entity with patient information (providers, plans, laboratories, pharmacies, etc.) can separately use information for marketing, and a patient opt-out is only effective against one institution at a time.

Adequacy

Will the HIPAA privacy rules be viewed as adequate under Article 26 of the European Union *Directive on the Protection of Individuals With Regard to the Processing of Personal*

¹⁹ 45 C.F.R. §164.512.

²⁰ 45 C.F.R. §164.512(f).

²¹ 45 C.F.R. §164.514(e) & (f).

*Data and on the Free Movement of Such Data?*²² Determinations of adequacy can be complex and require an evaluation of many factors. However, even a superficial review of the privacy rules suggests that it will be difficult to argue that the rules meet the EU standards. Problems include, but are not limited to:

- The mandatory consent provision for treatment, payment, and health care operations is inconsistent with Article 8 of the Directive, which requires explicit consent for the processing of sensitive information.

- The rules allow many uses and disclosures of sensitive health information without the effective consent of the data subject. The use of health data for marketing without consent or even a meaningful opt-out is the most telling example. The marketing provision is inconsistent with the provisions of Article 14 relating to the right to object to the processing of data for marketing.

- The limited scope of the HIPAA rules and the narrow onward transfer provision mean that some health data covered by the rules can be transferred to others and escape the privacy protections of HIPAA. The business associate rule helps, but the rule does not apply to all data transfers. The HIPAA rule does not meet the onward transfer principles of the Directive.

- HIPAA provides no individual remedies. The Secretary of Health and Human Services will accept complaints and can investigate and punish covered entities that violate the privacy rules. However, the Secretary cannot award damages to individuals, and the HIPAA statute does not provide for an individual right to sue. Remedies may be available under state laws or common law.

Conclusion

The HIPAA privacy rules represent the first broadly applicable health privacy standards in the United States. Some parts of the rules offer new rights to individuals that exceed anything available under most state laws. To this extent, at least, the HIPAA rules will provide additional privacy protections. However, the rules have some considerable limitations and drawbacks. Some parts of the rule will actually undermine existing protections. The HIPAA rules may be sufficiently inconsistent with international privacy standards that they might easily be dismissed as insufficient to satisfy requirements of EU law and the law in other nations.

The HIPAA privacy rules remain a work in progress. Although the rules are final, they will change in the near future before compliance is required. It is highly unlikely that the problems identified in this short analysis will be resolved in favor of privacy, and it is possible that some changes will make things worse. One may hope, however, that at least some of the changes will result in improvements in privacy protections for data subjects who use the American health care system.

²² Council Directive 95/46/EC, 1995 O.J. (L 281) 31, at http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm.