Order Code RS20934
Updated August 27, 2002

A Brief Summary of the Medical Privacy Rule

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

This report provides a brief overview of the recently modified medical privacy rule, "Standards for the Privacy of Individually Identifiable Health Information"("privacy rule") published on August 14, 2002 by the Department of Health and Human Services (HHS). Issuance of the modified privacy rule by the Bush Administration is the culmination of a decades long debate over access to medical records that has pitted privacy advocates and civil libertarians against employers and much of the health care industry. As required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), privacy recommendations were made to Congress by HHS in 1997, and a privacy rule was issued by the Clinton Administration in December 2000. The privacy rule went into effect April 14, 2001, with compliance required by April 2003 for most entities. The regulation creates a new federal floor of privacy protections while leaving in place more protective state rules or practices. The rule establishes a set of basic consumer protections and a series of regulatory permissions for uses and disclosures of protected health information.

Background. In recent years, our society has come to rely increasingly on medical information to perform basic functions and to make decisions about individuals. However, a number of fundamental developments have threatened the confidentiality of health-care information, and are the cause of a great deal of concern. The emergence of third-party payment plans; the use of health-care information for non-health care purposes; the growing involvement of government agencies in virtually all aspects of health care; and the exponential increase in the use of computers and automated information systems for health record information have combined to put substantial pressure on traditional confidentiality protections. In addition, an increasing number of parties involved in health care treatment, payment, and oversight have routine access to personally identifiable health records. Greater utilization of health-care information coupled with inadequate confidentiality protections has increased the potential for unauthorized uses and disclosures of medical information. The disclosure of personally identifiable health-care information can profoundly affect people's lives. "It affects decisions on whether they are hired or fired; whether they can secure business licenses, and life insurance; whether they are permitted to drive cars; whether they are placed under police surveillance or labeled a security risk; or even whether they can get nominated for

and elected to political office."[1] Other secondary uses of health-care information, such as the use of genetic test results for employment and insurance purposes, have the potential to result in harm to the health-care subject if the information is disclosed for unauthorized purposes. These factors accentuate the need for strong legal safeguards.

Medical Privacy Laws. The confidentiality of health-care information is governed by various federal, state, and local statutes, ordinances, regulations, and case law. Also applicable are private accreditation standards, such as those of the Joint Commission on Accreditation of Healthcare Organizations, internal policies of particular institutions, and ethical guidelines of professional organizations. Prior to the issuance of the HIPAA privacy rule, federal laws did not address the confidentiality of health-care information collected and maintained by the private sector (*i.e.*, doctors, hospitals, health plans, health insurers, and other health-care related entities). A major impetus for the enactment of HIPAA's privacy requirement was the absence of a comprehensive federal law that protected the confidentiality of patient records in all settings.

Another impetus for the enactment of HIPAA was the lack of uniformity among the states in their treatment of the confidentiality of health-care information. There is substantial variation between the states on many aspects of medical records law. These differences are becoming much more critical in the collection, maintenance, and disclosure of health-care information as it is transmitted through interstate commerce amongst patients, physicians, health-care facilities, employers, government agencies, and insurers located in different states and subject to different laws. To address this disparity, HIPAA provides that state law, except for certain specified laws (concerning public health surveillance) and state laws that are more stringent, is preempted by the federal privacy rule. A compendium of state laws issued July 20, 1999 and updated July 2002 by Georgetown University's Health Privacy Project, "The State of Health Privacy: An Uneven Terrain", identifies medical records privacy provisions from state legislative codes. The report covers only state statutes and divides them by patient access, restrictions on disclosure, privilege, and condition specific requirements.[2]

The enactment of the European Union (EU) Data Privacy Directive in October, 1995, provided further impetus for congressional action. Article 25 of the Directive requires EU member states to enact laws that prohibit the transfer of personal data to non-EU countries that lack an "adequate level of protection." Determinations of adequacy are to be made by the European Commission. If a finding of inadequacy is made, EU member states must block transfers of personal data to that third country. In order to prevent the blockage of data transfers from the EU to the United States, the Department of Commerce entered into a safe harbor agreement with the EU to enable United States companies to meet the "adequacy" requirements. For further information, see CRS Report RS20823, *The EU-U.S. "Safe Harbor" Agreement on Personal Data Privacy.*

HIPAA. Several comprehensive medical records confidentiality bills were introduced during the past decade, with the end result being passage of the medical privacy requirements as part of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Health Insurance Portability and Accountability Act of 1996

---

[1] A. Westin, *Computers, Health Records, and Citizen's Rights* 60 (1976).

[2] See, [http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm].

(HIPAA), Pub. L. 104-191, 42 U.S.C. §§ 1320d *et seq.*, was created to improve the portability and continuity of health insurance coverage, to combat waste, fraud and abuse in health care, to promote the use of medical savings accounts, to improve access to long term care, and to simplify the administration of health insurance. Sections 261 through 264 of HIPAA are known as the administrative simplification provisions. The general administrative simplification rule requires health care payers and providers who transmit transactions electronically to use standardized data elements to conduct financial and administrative transactions. Section 262 directs HHS to issue standards to facilitate the electronic exchange of information, and to develop standards to protect the security of such information. Section 264 of HIPAA requires HHS to submit to the Congress detailed recommendations on standards with respect to the privacy rights that an individual who is the subject of individually identifiable health information should have, the procedures that should be established for the exercise of such rights, and the uses and disclosures of such information that should be authorized or required.

The Secretary made preliminary privacy recommendations to Congress September 1997, based on the core fair information principles of notice, consent, access, security, and enforcement/redress, to: limit the use of an individual's health care information to health purposes only; require organizations to provide adequate security measures to protect information from misuse or disclosure; provide patients with new rights to control how their health information is used, such as the ability to get copies of records and propose corrections; hold those who misuse personal health information accountable, and provide redress for persons harmed by its misuse through criminal and civil penalties; and balance privacy protections with public responsibility to support national priorities, including public health, research, quality care, and reduction of fraud and abuse, including allowing law enforcement access to personal health information.

In the 106th Congress several proposals to protect health information were considered, but Congress did not pass legislation. None of the bills were reported out of committee, with disagreements over the patient's right to sue, parental notification of minor's access to health care, and preemption precluding agreement. In the absence of the enactment of federal legislation, HIPAA required HHS to issue privacy regulations.

The December 2000 Privacy Rule. The final privacy regulation was published in the *Federal Register* on December 28, 2000 at 65 Fed. Reg. 82462, shortly before the Clinton Administration left office, and after HHS received over 52,000 comments on its initial proposal. Its original effective date of February 26, 2001 was subsequently changed to April 14, 2001.[3] Enforcement of the rule begins in April 2003, except for small health plans (annual receipts of $5 million or less) who have until 2004 to comply. The medical privacy rule prohibits covered entities from disclosing protected health information to any third parties, unless the rules otherwise permit the disclosure.

Applicability. The rule covers health plans, health care providers, and health care clearinghouses (entities that process or facilitate the processing of nonstandard data elements of health information into standard data elements). It only covers information

---

[3] 66 Fed. Reg. 12433 (Feb. 26, 2001)(the delayed effective date occurred as a result of HHS' failure to submit the rule to Congress for the required 60-day review period until February 13, 2001); *see also* 5 U.S.C. § 801(a)(1).

that is electronically transmitted or maintained. It covers protected health information in any form, whether oral, written or electronic.

Individual Rights. Individuals are given a right of access to their health information, a right to receive notice of the covered entity's privacy policies, a right to request amendments of their information, a right to an accounting of the disclosures made, and a right to file complaints regarding use or disclosure of their information. Individuals may request that restrictions be placed on the disclosure of their health information.

Permitted Uses and Disclosures With Consent or Authorization. The use of protected health information for treatment, payment, or health care operations (a provider's or health plan's management and other activities necessary for support of treatment or payment) requires the prior written consent of a patient. Disclosures for purposes other than treatment, payment, and health care operations require a prior written authorization.

Permitted Uses and Disclosures Without Consent or Authorization. Certain public priority uses and disclosures of information do not require prior written consent or authorization (such as health system oversight, public health activities, certain research activities, law enforcement, judicial and administrative proceedings, emergency treatment, and imminent threats to the health or safety of any person). Covered entities are permitted to disclose information to law enforcement for purposes of health care oversight (i.e., investigations of health care fraud, government program fraud, and civil rights investigations), for general law enforcement investigations (i.e., in response to grand jury subpoenas and court orders), to avert a serious threat to health and safety, to coroners and medical examiners, for investigations involving abuse (including child abuse), neglect, or domestic violence.

Information Practices. Disclosures of protected health information other than for treatment purposes must use only the "minimum necessary" information. Covered entities must enter into contracts with "business associates" requiring them to protect individual health information, and must take action if they know of practices by their business associates that violate the contractual agreement. Covered entities must adhere to specific procedures in using information for fundraising or marketing. There are special requirements that apply to both federal and privately funded research. Psychotherapy notes may not be used or disclosed to others without explicit authorization.

Preemption. State law, except for certain specified laws (concerning public health surveillance) and state laws that are more stringent, is preempted by the federal rule.

Enforcement. The Secretary, covered entities, and others are required to ascertain compliance with, and enforcement of the privacy regulation. Any person may file a complaint with the HHS Office for Civil Rights. In cases of noncompliance, the Secretary is directed to resolve the matter by informal means. If the matter cannot be resolved informally, the Secretary may issue written findings of non-compliance that may be used as a basis for initiating action (civil monetary penalties) or a criminal referral.

Penalties. Violators will be subject to civil monetary penalties ($100 per violation up to $25,000 per year), and criminal penalties (up to $250,000 and imprisonment up to 10 years) against covered entities that knowingly and improperly disclose identifiable health information. The regulation does not authorize patients to sue.

The final privacy rule was criticized by some for its complexity, and for the imposition of substantial administrative and financial burdens on the health care industry. At the same time, the regulation was applauded by privacy advocates, consumer groups, and some health care industry participants. The General Accounting Office found that considerable uncertainty existed regarding the actions needed to comply with the new privacy regulations. Major concerns among stakeholder groups and the Congress centered on consent and authorization procedures; contractual liability and business associates; parental access to minors' health information (typically related to substance abuse, mental health treatment, and reproductive care); preemption of state laws; law enforcement access to protected health information; costs; and technical assistance.

The August 2002 Privacy Rule. The Bush Administration and HHS re-opened the privacy rule to additional comment on February 8, 2001,[4] and announced that it would accept further comments on the rule until March 30, 2001, see 66 Fed. Reg. 12378. The scope and cost of the rule, coupled with the substantial nature of some concerns raised in the initial comment period, led HHS to conclude that an additional comment period was warranted. On April 12, 2001, Secretary Thompson announced that HHS would immediately begin the process of implementing the patient privacy rule, of issuing guidelines, and of considering any necessary modifications. Several areas were targeted for clarification or modification: impediments to information sharing; consent and authorization procedures; parental access to minors' health information; uses and disclosures for treatment, payment, and health care operations; notices of privacy practices; minimum necessary uses and disclosures; oral communications; business associates; uses and disclosures for marketing; parents as the personal representatives of unemancipated minors; uses and disclosures for research purposes; uses and disclosures for which authorizations are required; and de-identification. On July 6, 2001 HHS issued interpretative guidance materials on the rule.[5] In response to numerous and extensive comments received by HHS, along with intense lobbying efforts by various stakeholders, in March 2002 the Bush Administration issued proposed modifications to the privacy rule in the *Federal Register* at 67 Fed. Reg. 14775, and permitted a 30-day comment period on its proposal. On August 14, 2002, HHS published in the *Federal Register* the privacy rule with certain modifications, 67 Fed. Reg. 53181. The August 2002 modification is virtually unchanged from the March 2002 proposal, does not require Congressional approval, and has the force of law. A summary of significant final modifications follows. For detailed discussion of medical privacy issues, see CRS Report RL30620, *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations*.

Notice. The August 2002 rule adds a new requirement for health care providers with a direct treatment relationship, that they make a good faith effort to obtain an individual's written acknowledgment of receipt of the provider's privacy notice.

---

[4] During the 12 month period after the standards are initially adopted, the Secretary is permitted to modify the standards only if necessary to permit compliance. After the first year of adoption, HHS may modify the standards not more than once every 12 months. Additions or modifications are to be completed in a manner that minimizes the disruption and costs. 42 U.S.C. § 1320d-3(b).

[5] Available at [http://www.hhs.gov/ocr/hipaa/finalmaster.html].

Consent and Authorization. The requirement for providers to obtain an individual's prior written consent to use or disclose protected health information for treatment, payment or health care operations was eliminated. The August 2002 rule permits covered entities to obtain consent, but does not require it. Although patient authorizations will still be required to use and disclose information for purposes outside of treatment, payment, and health care operations, the August 2002 rule standardizes the core requirements in authorization forms, and allows health care groups to use a single type of authorization to get permission to use information for a specific purpose or disclosure.

Minimum Necessary. The August 2002 rule exempts from the minimum necessary standards any uses or disclosures for which an authorization has been received.

Incidental Use and Disclosure. The August 2002 rule explicitly permits incidental disclosures resulting from activities such as discussions at nursing stations, the use of sign-in sheets, calling out names in waiting rooms, etc. provided reasonable safeguards and minimum necessary requirements are met.

Business Associates. The August 2002 rule allows covered entities, except small health plans, up to one year beyond the April 14, 2003 enforcement date to change existing contracts with business associates. Model business associate contract provisions are provided.

Marketing. The August 2002 rule requires covered entities to obtain prior patient authorization for marketing, except for a face-to-face communication or a communication involving a promotional gift of nominal value. The rule distinguishes between activities that are and are not marketing. The definition of "marketing" in the new rules excludes communications by a health care provider promoting its own goods and services.

Medical Information of Minors. The December 2000 privacy rule generally gives control of health information about a minor to the parent, guardian, or person acting in loco parentis. The August 2002 rule clarifies that state law governs in the area of parents and minors, and that HIPAA does not overturn state laws that give providers discretion to disclose or deny health information to parents.

Research. The December 2000 privacy rule provides that protected health information may not be used or disclosed for research without either a written authorization or a waiver of authorization approved by an Institutional Review Board or a Privacy Board. In the August 2002 rule, HHS significantly simplified the administrative burdens for obtaining authorizations and assessing requests for waivers of authorization.

Disclosures to Obtain Payment. The December 2000 rule prevents a provider from disclosing protected health information to another entity for other than treatment purposes. Under the August 2002 rule, a covered entity is permitted to disclose protected health information to other covered entities and to noncovered health care providers to enable the recipient to make or obtain payment. Protected health information may also be disclosed to another covered entity for specified operational purposes of the recipient, as long as both entities have a relationship with the individual.