Order Code RS20934
Updated April 10, 2002

A Brief Summary of the Medical Privacy Rule

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

On March 27, 2002 the Department of Health and Human Services (HHS) published its proposed changes to the medical privacy regulations issued by the Clinton Administration under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HHS is accepting comments on the proposed changes until April 26, 2002. This report provides an overview of the final rule for "Standards for the Privacy of Individually Identifiable Health Information" ("privacy rule") that went into effect on April 14, 2001, and an overview of the Bush Administration's proposed changes to the privacy regulation. Many of the proposed changes address problems identified by HHS in its guidance on the privacy rule issued July 2001. However, the proposed rule also contains a number of revisions that were not identified in the July 2001 guidance. Some changes are more significant than others. HIPAA expressly permits the HHS Secretary to modify any of its required standards, such as the privacy standard, after the first year, once every 12 months. There is no target date for the publication of the final rule, but it must be published by October 13, 2001 to meet the requirement that covered entities have 180 days to incorporate changes. The compliance deadline is April 2003. For detailed discussion of medical privacy issues, see CRS Report RL30620, *Health Information Security and Privacy: HIPAA and Proposed Implementing Regulations*.

On December 28, 2000, shortly before the Clinton Administration left office, HHS published the final rule on health information privacy, as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] HIPAA 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.[2] 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

[1] 65 Fed. Reg. 82462 (Dec. 28, 2000)(to be codified at 45 C.F.R. pt. 160 - 164 (Dec. 28, 2000) [http://aspe.hhs.gov/admnsimp/final/PvcTxt01.htm].

[2] 42 U.S.C. §§ 1320d *et seq.* (1994 & Supp. IV 1998).

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. HIPAA establishes timetables for the adoption, addition, and modification of the administrative simplification standards. HIPAA provides that, subject to limited exceptions, the Secretary shall review the standards, and adopt appropriate additions or modifications to the standards, not more frequently than once every 12 months.[3] Additions or modifications are to be completed in a manner that minimizes the disruption and cost of compliance. The Secretary is not permitted to modify any standard, except for the code sets standard, during the 12 month period beginning on the date that the standard is initially adopted "*unless the Secretary determines that the modification is necessary in order to permit compliance with the standard*." (emphasis added).[4] Modifications to any of the standards may be made after the first year, but not more than once every 12 months.

The Secretary made her preliminary privacy recommendations to Congress on September 11, 1997.[5] In the 106th Congress several proposals to protect health information were considered, but Congress did not pass legislation.[6] 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 final privacy regulations. The final privacy regulation was published on December 28, 2000 after HHS received over 52,000 comments on its initial proposal.

The final regulation issued in December 2000 was intended to create a new federal floor of privacy protections that leaves in place more protective state rules or practices. It describes a set of basic consumer protections and a series of regulatory permissions for use and disclosure of protected health information. HHS estimates that the 10-year costs of implementing the privacy regulation will be $17.6 billion, offset by $29 billion in savings over 10 years from the transaction and code set rule required by HIPAA. Net savings for the two rules are forecast to be $12.3 billion. The final regulation applies to a specified set of entities, referred to as covered entities: health plans, health care clearinghouses (entities that process or facilitate the processing of nonstandard data elements of health information into standard data elements), and health care providers who transmit any health information in electronic form in connection with an administrative simplification transaction. Entities covered by the health information privacy rule have until April 2003 to comply, with the exception of small health plans (those with annual receipts of $5 million or less) who have until 2004 to comply.

---

[3] 42 U.S.C. § 1320d-3(b).

[4] *Id.*

[5] Confidentiality of Individually-Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996. [http://aspe.os.dhhs.gov/admnsimp/pvcrec.htm].

[6] See CRS Archived Issue Brief IB98002, *Medical Records Confidentiality*, by Harold Relyea, Stephen Redhead, and Gina Stevens.

The regulations cover all protected health information in any form, whether oral, written or electronic. The use of protected health information for treatment, payment, or health care operations[7] requires the prior **written consent** of a patient, except in certain circumstances. Uses and disclosures of protected health information for purposes other than treatment, payment, and health care operations require a prior detailed and explicit **written authorization** from the individual. Entities covered by the regulation must enter into contracts with "**business associates**" requiring them to protect individual health information. Covered entities must take action if they know of practices by their business associates that violate the contractual agreement. Most disclosures of protected health information other than for treatment must use only the "**minimum necessary**" information. Covered entities must adhere to specific procedures in using information for fundraising or **marketing**. The regulation also establishes special requirements for use of protected health information that apply to both federal and privately funded **research**. 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. Psychotherapy notes may not be used by, or disclosed to others without explicit authorization. Exceptions to the consent and authorization requirements are provided for certain public priority uses of information, 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. State law, except for certain specified laws (concerning public health surveillance) and state laws that are more stringent, is preempted by the federal rule.

The Secretary, covered entities, and others are required to ascertain compliance with, and enforcement of the privacy regulation.[8] The Secretary is to seek the cooperation of covered entities in obtaining compliance with the regulation, and is authorized to provide technical assistance to covered entities to help them comply voluntarily. The regulation permits any person to file a complaint with the HHS Office for Civil Rights if the person believes a covered entity is not complying with the rule. The regulation provides that the Secretary may investigate such complaints. The regulation also authorizes the Secretary to conduct compliance reviews. Covered entities are required to provide records and compliance reports, to cooperate with complaint investigations and compliance reviews, and to permit access to information. In cases where a compliance review indicates a failure to comply, the Secretary is directed to resolve the matter by informal means whenever possible. If the matter cannot be resolved informally, the Secretary may issue written findings documenting the non-compliance. The non-compliance findings may be used as a basis for initiating action (civil monetary penalties) or initiating a criminal referral (penalties for disclosing individually identifiable health information). 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

---

[7] Health care operations are a provider's or health plan's management and other activities necessary for support of treatment or payment.

[8] *See* 65 Fed. Reg. at 82801-2.

regulation does not authorize patients to sue to enforce the privacy standards. However, a patient may bring a claim in a state where such actions are permitted.

The final privacy rule was criticized for its complexity, and for the imposition of substantial administrative and financial burdens on health care industry participants.[9] At the same time, the regulation was applauded by privacy advocates, consumer groups, and some health care industry participants.[10] The General Accounting Office ("GAO") testified that "considerable uncertainty remains regarding the actions needed to comply with the new privacy regulations."[11] Concern among the stakeholder groups centered on conditions for consent, authorization, and disclosures; rules pertaining to the business associates of covered entities; limited preemption of state laws; the costs of implementation; and HHS' capacity to provide technical assistance. Some members of Congress were concerned about particular aspects of the privacy rule. House Ways and Means Committee Chairman William M. Thomas and Health Subcommittee Chairwoman Nancy L. Johnson recommended that the provision requiring providers to obtain consent to use and disclose patient health care information for treatment, payment and health care operations be eliminated, along with the business associate provision to avoid potential contract liability. Representative Edward Markey and several other members asked President Bush not to modify several of the regulation's provisions. Senate Health, Education, Labor and Pensions Chairman Edward M. Kennedy and Senate Judiciary Committee Chairman Patrick J. Leahy were included in this group. They recommended that the consent provision be maintained, and also expressed support for the provision requiring covered entities to enter into contracts with business associates. Support was also expressed for the provision that permits health care providers not to disclose protected health information to the parents of minor children when state laws, typically related to substance abuse, mental health treatment, and reproductive care, permit minors to access health care without parental consent.

When the final rule was published it had an effective date of February 26, 2001. However, HHS subsequently established a later effective date of April 14, 2001.[12] On February 8, 2001, HHS announced that it would accept further comments on the rule up until March 30, 2001.[13] In this notice, HHS stated that the scope and cost of the rule, coupled with the substantial nature of some concerns raised in the initial comment period, led it to conclude that an additional comment period was warranted. HHS Secretary

---

[9] *See Making Patient Privacy a Reality: Does the Final HHS Regulation Get the Job Done? Hearing Before the Senate Comm. On Health, Education, Labor, and Pensions*, 107th Cong. (Feb. 8, 2001).

[10] *Id.*

[11] *See Health Privacy: Regulation Enhances Protection of Patient Records but Raises Practical Concerns, Testimony of U.S. General Accounting Office before the Senate Comm. On Health, Education, Labor, and Pensions*, 107th Cong. (Feb. 8, 2001).

[12] 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 resulting in the establishment of a new effective date 60 days later – April 14, 2001); *see* 5 U.S.C. § 801(a)(1); *see also* CRS Report RL30116, *Congressional Review of Agency Rulemaking: A Brief Overview and Assessment After Five Years*, by Morton Rosenberg (2001).

[13] 66 Fed. Reg. 12378 (Feb. 28, 2001).

Thompson indicated that the Department would "review the comments it receives to determine whether changes in the final rule are needed."[14] On April 12, 2001, Secretary Thompson announced that HHS would immediately begin the process of implementing the patient privacy rule, and of issuing guidelines on how the rule should be implemented in order "to clarify some of the confusion regarding the impact the rule might have on health care delivery and access" and also "consider any necessary modifications that will ensure the quality of care does not suffer inadvertently from this rule."[15] The Secretary highlighted several areas targeted for clarification or modification: "that doctors and hospitals will have access to necessary medical information about a patient they are treating and they will be able to consult with other physicians and specialists regarding a patient's care; patient care will be delivered in a timely and efficient manner and not unduly hampered by the confusing requirements surrounding consent forms; and parents will have access to information about the health and well-being of their children, including information about mental health, substance abuse or abortion."[16] The areas of concern focus on impediments to information sharing, involve consent and authorization procedures, or relate to parental access to minors' health information. On July 6, 2001 HHS issued guidance materials to explain and clarify key provisions of the rule.[17]

On March 27, 2002, HHS Secretary Tommy G. Thompson published proposed changes to HHS' health privacy regulations.[18] There are several proposed changes to the privacy rule, with some changes more significant than others. A significant change in the proposed rule would eliminate the requirement for providers to obtain, prior to using or disclosing protected health information, an individual's written **consent** for treatment, payment or health care operations. Under the proposed rule, covered entities would be permitted to obtain consent, but would not be required to. The proposed rule adds a new requirement that health care providers with a direct treatment relationship must make a good faith effort to obtain an individual's written acknowledgment of receipt of the provider's notice of privacy practices. Other covered entities, such as health plans, would not be required to obtain the acknowledgment.

Another proposed change relates to **disclosures to another entity for payment and operations**. The current rule prevents a provider from disclosing protected health information to another entity for other than treatment purposes. Under the proposed rule, a covered entity would be permitted to disclose protected health information to other covered entities, and to noncoverd health care providers, to enable the recipient to make or obtain payment. Protected health information, under the proposal, 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. The proposal clarifies that

---

[14] *See* "Statement by HHS Secretary Tommy G. Thompson," U.S. Department of Health and Human Services, Feb. 23, 2001. [http://www.hhs.gov/news/press/2001pres/20010223.html].

[15] *See* "Statement by HHS Secretary Tommy G. Thompson," U.S. Department of Health and Human Services, Apr. 12, 2001. [http://www.hhs.gov/news/press/2001pres/20010412.html].

[16] *Id.*

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

[18] 67 Fed. Reg. 14775 (March 27, 2002) [http://www.hhs.gov/ocr/hipaa/propmods.txt].

covered entities participating in an organized health care arrangement may share protected health information for health care operations.

Another focus of the proposed rule is the **minimum necessary** requirement which limits the use and disclosure of protected health information for payment or health care operations to the minimum necessary to accomplish the intended purpose. In HHS' guidance to the privacy rule, it states that the minimum necessary requirement was a reasonableness standard, and that covered entities have flexibility to make their own assessments of what information is reasonably necessary for particular purposes. This statement is repeated in the commentary to the proposed rule, but no changes are recommended to the final rule in this area. With respect to **oral communications**, the privacy rule protected the disclosure of health information through oral communication. The proposed rule retains the oral communications requirement, but would explicitly permit incidental disclosures resulting from activities such as discussions at nursing stations, the use of sign-in sheets, calling out names in waiting rooms, etc.

Another area of concern in the privacy rule was the provision that permits a covered entity to disclose protected health information to a **business associate** who performs a function on behalf of the covered entity so long as the covered entity enters into a contract with the business associate specifying safeguards. The proposed rule would allow covered entities to continue to operate under existing contracts with business associates for up to one year beyond the April 14, 2003 compliance date. Covered entities would still be required to comply with the patient rights obligations commencing on April 14, 2003. An appendix offers model business associate contract provisions. Although patient **authorizations** would still be required to use and disclose information for purposes outside of treatment, payment, and health care operations, the proposed rule would standardize the core requirements in the authorization forms, and allow health care groups to use a single type of authorization to get a patient's permission to use information for a specific purpose or disclosure. The final privacy rule generally does not permit covered entities to use or disclose protected health information for **marketing** products or services that are not health-related, without the express authorization of the individual. The proposed rule would require covered entities to obtain an authorization from the individual before making any marketing communications. The proposed rule also clarifies the definition of "marketing."

The privacy rule generally gives control of health information about a **minor** to the parent, guardian, or person acting in loco parentis. This is not the case where state law or a court allows the minor, or someone other than the parent to consent to treatment. The proposed rule would continue to defer to state law, but clarifies that HIPAA does not overturn state laws that give providers discretion to disclose health information to parents, or that prohibit disclosure of health information to a parent. With respect to the use and disclosure of health information for **research**, the 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 proposed rule, HHS significantly simplified the administrative burdens for obtaining authorizations and assessing requests for waivers of authorization.