Order Code RS20500
Updated January 3, 2003

Medical Records Privacy: Questions and Answers on the HIPAA Final Rule

C. Stephen Redhead
Specialist in Life Sciences
Domestic Social Policy Division

Summary

On December 28, 2000, the Secretary of Health and Human Services (HHS) issued a final regulation to protect the privacy of personally identifiable medical information. Modifications to the privacy rule were published on August 14, 2002. The modified final rule, which covers health care providers, health plans, and clearinghouses, gives patients the right to inspect, copy and, in some cases, amend their medical records. Covered entities are permitted to use and disclose health information for routine health care operations and for various specified national priority activities (e.g., law enforcement, public health, research). They are required to have in place reasonable safeguards to protect the privacy of patient information and limit the information used or disclosed to the minimum amount necessary to accomplish the intended purpose of the use or disclosure. Health plans and providers must obtain a patient's prior written authorization to use or disclose information for most other purposes. Covered entities that fail to comply with the rule are subject to civil and criminal penalties, but patients do not have the right to sue for violations of the law. The health privacy rule does not preempt, or override, state laws that are more protective of medical records privacy. The compliance deadline for most covered entities is April 14, 2003.

Introduction

On December 28, 2000, the Secretary of Health and Human Services (HHS) issued a comprehensive final regulation to protect the privacy of medical records and other personal health information. HHS published significant modifications to the regulation on August 14, 2002. The health privacy rule gives patients the right to access and copy their medical records, limits the use and disclosure of personal health information without a patient's written authorization, and requires health plans and health care providers to provide patients with a written notice describing the types of permissible uses and disclosures of their medical information. It also restricts most disclosures of health information to the minimum needed for the intended purpose, and establishes new financial penalties for improper use or disclosure of personal health information.

The health privacy rule is one of several new standards mandated by the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, P.L. 104-191, 42 U.S.C. 1320d). Congress enacted those provisions in an attempt to streamline the administration of health information as the health care industry moves towards electronic record keeping and claims processing. The intent of the legislation is to reduce paperwork, lower administrative costs, safeguard the security of health information, and facilitate the networking and coordination of health information and health care activities.

HIPAA instructed the Secretary to issue regulations to establish standard electronic formats for certain specified financial and administrative transactions (e.g., verifying insurance coverage, claims for payment), and to require uniform data codes for reporting diagnoses, referrals, authorizations, and medical procedures. The Secretary is also required to develop security standards to safeguard confidential health information against unauthorized access, use, and disclosure. Finally, HIPAA instructed the Secretary to develop standards for unique identifiers (i.e., ID numbers) for patients, employers, health plans, and health care providers.

The growing use of networked, electronic health information has raised serious privacy concerns among the public. Patients are increasingly worried about who has access to their medical information without their express consent. They fear that their personal health information will be used to deny them employment or insurance. Lawmakers addressed these concerns by adding privacy language to HIPAA, after failing to pass stand-alone health privacy legislation. HIPAA gave Congress until August 21, 1999, to enact comprehensive health privacy legislation, otherwise the Secretary was instructed to issue a health privacy regulation by February 21, 2000. When Congress missed its self-imposed deadline, the Secretary proposed health privacy standards in November, 1999, and published the final rule on December 28, 2000. Most covered entities must be in compliance by April 14, 2003.

Questions and Answers about the Health Privacy Rule

Who is Covered? As specified under HIPAA, the privacy regulation applies to three groups of entities: (i) individual and group health plans that provide or pay for medical care; (ii) health care clearinghouses (i.e., entities that facilitate and process the flow of information between health care providers and payers); and (iii) health care providers who transmit health information electronically in a standard format in connection with one of the HIPAA-specified transactions, or who rely on third-party billing services to conduct such transactions. The rule, therefore, does not apply directly to other entities that collect and maintain health information such as life insurers, researchers, employers (unless they are acting as providers or plans), and public health officials. However, business associates with whom covered entities share health information are covered. Business associates include persons who provide legal, actuarial, accounting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity. The rule permits a covered entity to disclose health information to a business associate or to allow the business associate to create or receive health information on its behalf, provided both parties sign a written contract that essentially binds the business associate to the covered entity's privacy practices.

What Type of Health Information is Covered? The rule covers all individually identifiable health information that is created or received by a covered entity, including genetic information and information about an individual's family history. It applies to both paper and electronic records, as well as oral communications. Non-identifiable health data, from which all personal identifiers have been removed, are not subject to the rule.

Can Patients Access and Amend their Health Information? Yes, covered entities must allow patients to inspect or obtain a copy of their health information, except in certain limited circumstances. Covered entities may charge a reasonable, cost-based copying fee. Patients may also request amendment or correction of information that is incorrect or incomplete. Finally, patients have the right to receive a detailed accounting of certain types of disclosures of their health information made by covered entities during the past 6 years. Disclosures for routine health care operations and those made pursuant to an authorization (see below) are exempt from the accounting requirement.

Does the Use and Disclosure of Health Information by Covered Entities Require a Patient's Authorization? The privacy rule imposes certain restrictions on when and how covered entities may use and disclose individually identifiable health information.[1] Covered entities may use and disclose health information for treatment, payment, and other routine health care operations (TPO) without the individual's permission and with only a few restrictions. Patients have the right to request that covered entities restrict the use and disclosure of their health information for TPO. Covered entities are not required to agree to such a request. Covered entities may also disclose certain information to a family member, relative, close friend, or other person identified by the patient, provided the patient is given the opportunity to agree or object (opt out). If the patient is not present, covered entities may use their professional judgement in deciding whether a disclosure is appropriate. Thus, a pharmacist may allow a family member to pick up a prescription on behalf of the patient.

The privacy rule also permits the disclosure of health information without a patient's authorization for various specified national priority activities, consistent with other applicable laws and regulations. First, disclosures may be made for **public health** purposes (e.g., reporting diseases, collecting vital statistics), as required by state and federal law. Second, health information may be disclosed to public agencies to conduct **health oversight** activities such as audits; inspections; civil, criminal, or administrative proceedings; and other activities necessary for oversight of the health care system. Third, disclosures may be made to **law enforcement** officials pursuant to a warrant, subpoena, or order issued by a judicial officer, or pursuant to a grand jury subpoena. Disclosures for law enforcement purposes are also permitted pursuant to an administrative subpoena or summons where a three-part test is met (i.e., the information is relevant, the request is specific, and non-identifiable information could not reasonably be used). Fourth, health information may be disclosed in **judicial and administrative proceedings** if the request

---

[1] For the most part, the privacy rule addresses *permissible* uses and disclosures. HHS expects covered entities to rely on their professional judgement in deciding whether to permit the use or disclosure of health information covered under the rule. Covered entities are *required* to disclose information only to the individual who is the subject of the information and to HHS for enforcement of the regulation.

for the information is made through or pursuant to a court order. Fifth, covered entities may disclose health information to **researchers** without a patient's authorization, provided an Institutional Review Board (IRB) or an equivalent, newly formed "privacy board" reviews the research protocol and waives the authorization requirement.[2]

Health information may also be disclosed without authorization: (i) to coroners, medical examiners, and funeral directors; (ii) to workers' compensation programs; (iii) to a government authority authorized to receive reports of abuse, neglect, or domestic violence; (iv) to organizations in order to facilitate organ, eye, and tissue donation and transplantation; (v) to government agencies for various specialized functions (e.g., national security and intelligence activities); (vi) to avert a serious threat to health or safety; (vii) and in other situations as required by law.

Covered entities must obtain a patient's specific authorization in writing for uses and disclosures of health information that are not otherwise required or permitted by the privacy rule (e.g., releasing information to financial institutions that offer mortgages and other types of loans, or selling mailing lists to marketing companies). All authorization forms must contain certain specified core elements including a description of the health information to be used or disclosed and the identity of the recipient of the information. In general, a covered health care provider may not condition the provision of treatment on receiving a patient's authorization. Health plans may condition enrollment or eligibility for benefits on the provision of an authorization prior to an individual's enrollment in the plan. Patients may in writing revoke their authorization at any time.

Are There Limits on the Amount of Information Disclosed? The rule requires that whenever a covered entity uses or discloses health information, or requests such information from another covered entity, it must make a reasonable effort to limit the information to the minimum amount necessary to accomplish the intended purpose of the use or disclosure. The minimum necessary standard does not apply to: treatment-related disclosures; disclosures made to patients upon their request; disclosures made to the Secretary to enforce compliance; any uses or disclosures for which the covered entity has received an authorization; and uses or disclosures that are required by law.

What about Incidental Disclosures? Incidental uses and disclosures of health information that occur as a result of a use or disclosure that is otherwise permitted by the privacy regulation are not considered violations of the rule, provided that the covered entity has met the reasonable safeguards and minimum necessary standards. Examples of incidental uses and disclosures include patient sign-in sheets, bedside charts, and confidential conversations that are inadvertently overheard by others.

Are Covered Entities Required to Explain their Privacy Practices to Patients? Yes, health plans and health care providers must provide patients with written notice of their privacy practices. Plans are required to give notice at enrollment.

---

[2] All federally funded research that involves human subjects, as well as clinical trials of new drugs and medical devices (regardless of the source of funding), are governed by a set of federal regulations called the Common Rule (45 CFR 46, Subpart A). Under the Common Rule, research proposals must be approved by an IRB, which decides whether or not to require informed consent based on the level of risk to the research subjects.

Providers that have a direct treatment relationship with the patient are required to give notice at the date of first service delivery and, except in emergency situations, make a good faith effort to obtain a written acknowledgment from the patient of receipt of the notice. The notice must include a description of the patient's rights, the legal duties of the covered entity, and a description of the types of uses and disclosures of information that are permitted, including those that do not require an authorization.

Does the Rule Restrict Employers' Access to Health Information? The rule permits a group health plan to disclose individually identifiable health information to an employer that sponsors the plan, provided the information is used only for plan administration purposes. In order for a group health plan to disclose health information to a plan sponsor, the plan documents must be amended so that they limit the uses and disclosures of information by the sponsor to those consistent with the privacy rule. In addition, an employer must certify to a group health plan that it will not use the information for employment-related actions (e.g., hiring and promotion decisions). The employer must agree to establish adequate firewalls, so that only those employees that need health information to perform functions on behalf of the group health plan have access to such information.

Is an Authorization Required to Disclose Information for Marketing? A covered entity may not disclose health information to a third party, in exchange for direct or indirect remuneration, for the marketing activities of the third party. However, health care-related communications made by covered entities are not defined as marketing under the rule and therefore do not require a patient's authorization. Such communications include prescription refill reminders, as well as information about alternative treatments, therapies, health care providers, and settings of care. More controversial communications are also excluded from the rule's definition of marketing. For example, communications from pharmacies, paid for by a drug manufacturer, that recommend that patients switch their medication to the company's product would not be considered marketing under the rule, and thus would not require prior authorization.

Are there Additional Privacy Protections for Psychotherapy Notes? Yes, psychotherapy notes (i.e., subjective notes recorded during counseling sessions) are held to a higher standard of protection, and patient authorization is required for almost all uses and disclosures. Health plans may not condition enrollment or eligibility for benefits on an individual's authorization for the release of psychotherapy notes.

What Must Covered Entities do to Ensure Compliance? Covered entities must have reasonable administrative, technical, and physical safeguards in place, commensurate with the size and scope of their business, to protect the privacy of patient information. These include designating a privacy official, training employees, and developing a system of sanctions for employees who violate the entity's policies. Covered entities are not directly liable for the actions of their business associates. They may be held liable if they know of a business associate's pattern of activity or practice in violation of the contract and they fail to take reasonable steps to correct the problem and, if such steps are unsuccessful, terminate the contract or report the problem to HHS.

Are there Penalties for Non-Compliance? HIPAA gave the Secretary the authority to impose civil monetary penalties against covered entities that fail to comply with the regulation, and criminal penalties for certain wrongful disclosures of personal

health information. The civil fines are $100 per incident, capped at $25,000 per year for each provision that is violated. The criminal penalties are graduated, depending on the offense, and include fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer or use it for commercial advantage, personal gain, or malicious harm.

Does the Rule Preempt State Health Privacy Laws? As mandated by HIPAA, the rule does not preempt, or override, state laws that are more protective of patient privacy. Although most states do not have comprehensive health privacy laws, many states have detailed, stringent standards governing the use and disclosure of health information related to certain medical conditions, such as mental illness, genetic testing, and communicable diseases (e.g., HIV/AIDS). These stronger privacy protections will remain in force. The rule only preempts state laws that are in conflict with its requirements and that provide less stringent privacy protections. Therefore, it serves as a federal "floor" of minimum privacy protections. On the controversial issue of parental notification, the rule defers to state law. Covered entities are allowed to disclose a minor's health information to a parent if such disclosure is permitted by state law. Similarly, disclosure to a parent is not permitted where prohibited by state law.

How Much Will it Cost to Implement the Rule? HHS estimates that implementing the privacy regulation will cost $17.5 billion over 10 years. According to the agency, this amount will be more than offset by the HIPAA electronic transactions and code sets standards, which are estimated to save the health care industry $29.9 billion over 10 years. Together, the two rules will produce a net savings of about $12.4 billion in improved health care efficiency and privacy protection.

What was the Reaction of Stakeholders to the Final Modified Rule? Patient privacy advocates strongly supported the December 2000 final rule. But they were very critical of the modifications to the rule, which eliminated the requirement that patients provide their one-time, written consent to use and disclose health information for TPO. Privacy advocates are also concerned that the modified rule will permit many of the aggressive drug marketing tactics that they claim are undermining patients' trust in the health care system. Finally, they remain concerned that HIPAA did not grant HHS the authority to cover all entities that handle medical information, nor did it give patients the right to sue for violations of their health information privacy.

Hospitals, health insurers, and other health care industry groups were generally pleased with the modifications to the rule, especially the elimination of the prior consent requirement, which they claim would have impeded routine health care operations and compromised patient care. However, at field hearings held by the National Committee on Vital and Health Statistics, health care industry representatives have called on the federal government to help providers and other covered entities to meet the April 2003 compliance deadline by issuing draft forms for authorization and notice of privacy practices, as well as detailed guidance regarding business associate relationships.

Where Can I Obtain More Information? Information on all the HIPAA standards can be found at [http://aspe.os.dhhs.gov/admnsimp]. HHS's Office of Civil Rights, which is responsible for implementing and enforcing the privacy rule has established a privacy home page at [http://www.hhs.gov/ocr/hipaa].