Order Code RS20500
Updated February 4, 2005

Medical Records Privacy: Questions and Answers on the HIPAA Rule

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

Summary

The HIPAA privacy rule gives patients the right of access to their medical information and prohibits health plans and health care providers from using or disclosing individually identifiable health information without a patient's written authorization except as expressly permitted or required by the rule. Plans and providers are permitted to use and disclose health information for treatment, payment, and other routine health care operations and for various specified national priority activities (e.g., law enforcement, public health, research). Providers may also share certain information with family members and others, as long as the patient is given the opportunity to object. Health plans and providers must give enrollees and patients a notice explaining their privacy rights and how their information will be used. They are also required to have in place reasonable safeguards to protect the privacy of patient information and, in general, must limit the information used or disclosed to the minimum amount necessary to accomplish the intended purpose of the use or disclosure. Entities that fail to comply with the rule are subject to civil and criminal penalties, but patients do not have the right to sue in federal court for violations of the rule. The privacy rule does not preempt, or override, state laws that are more protective of medical records privacy.

Introduction

Health plans and health care providers and their business associates are subject to the federal health information privacy regulation (45 CFR Parts 160, 164). The privacy rule gives patients the right of access to their medical information and prohibits health plans and health care providers from using or disclosing individually identifiable information without a patient's written authorization except as expressly permitted or required by the rule. For routine health care operations, including treatment and payment, plans and providers may use and disclose health information without the individual's authorization. In certain other circumstances (e.g., disclosures to family members and friends), the rule requires plans and providers to give the individual the opportunity to object to the disclosure. The rule also permits the use and disclosure of health information without the individual's permission for various specified activities (e.g., public health oversight, law enforcement) that are not

directly connected to the treatment of the individual. For uses and disclosures that are not permitted by the rule, plans and providers must obtain a patient's written authorization. They must also have in place reasonable administrative, technical, and physical safeguards to protect patient information from intentional or unintentional uses or disclosures that are in violation of the rule.

The health privacy rule is one of several new standards mandated by the 1996 Health Insurance Portability and Accountability Act (HIPAA) to support the growth of electronic record keeping and claims processing in the nation's health care system. Under HIPAA, the Secretary of Health and Human Services (HHS) has issued electronic format and data standards for several routine administrative transactions between plans and providers (e.g., claims for payment). The Secretary has also issued security standards to safeguard electronic patient information against unauthorized access, use, and disclosure. Most plans and providers have until April 21, 2005, to comply with the security standards.

The HIPAA privacy and security standards have helped lay the groundwork for the adoption of information technology (IT) systems in health care to support the electronic collection and exchange of patient information. Developing a secure platform to protect confidential health information is central to the growth of a national health information infrastructure that allows health care providers to share patient information. A small but growing number of communities and health care systems around the country have developed electronic medical records and established secure networks for the exchange of health data among providers, patients, and other authorized users. The creation of regional networks is seen as a critical step toward the goal of interconnecting the health care system nationwide. The handling of electronic patient information by these networks has important and, as yet, not fully understood implications for the privacy rule, which was developed with the traditional paper-based system of medical records in mind.

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 Types of Health Information Are Covered? The rule covers all individually identifiable health information that is created or received by a covered entity, including genetic tests and information about an individual's family history. It applies to

both paper and electronic records, as well as oral communications. Health information from which all personal identifiers have been removed is 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 six years. Disclosures for routine health care operations and those made pursuant to an authorization (see below) are exempt from the accounting requirement.

How May Plans and Providers Use and Disclose Patient Information? The privacy rule places certain limitations on when and how health plans and health care providers may use and disclose medical information. Generally, plans and providers may use and disclose health information for their own **treatment, payment, and health care operations (TPO)** without the individual's authorization and with few restrictions. A covered entity may also disclose information for: the treatment and payment activities of another provider; the payment activities of another health plan; and for certain health care operations of another covered entity, if each entity has a relationship with the patient. For example, a physician can mail or fax medical test results or a patient's medical record to a specialist who intends to treat the patient, provided that "reasonable safeguards" are used. Patients may request that covered entities restrict the use and disclosure of their information for TPO, but covered entities are not required to agree to such a request.

The privacy rule also permits the disclosure of health information without a patient's authorization for the following 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 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.[1]

---

[1] 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 Part 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.

Additionally, health information may 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.

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 entities are *required* to disclose information only to the individual who is the subject of the information and to HHS for enforcement of the rule. For all uses and disclosures of health information that are not otherwise required or permitted by the rule, covered entities must obtain a patient's written authorization (e.g., releasing information to financial institutions that offer mortgages and other types of loans, or selling mailing lists to marketing companies).

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 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.

Can Medical Information Be Shared with a Patient's Family or Friends? Yes, the rule permits covered entities to disclose information to a family member, relative, close friend, or other person identified by the individual. Only information that is directly relevant to such person's involvement with the individual's care may be shared. If the individual is present and able to make health care decisions, the covered entity may disclose information provided (1) the patient has been given, in advance, the opportunity to object to any disclosures, or (2) the covered entity, using professional judgment, reasonably infers that the patient does not object. In an emergency situation or if the patient is not present, the covered entity may use its professional judgment and experience with common practice in deciding whether a disclosure is appropriate. HHS has repeatedly stated that it is not the intent of the rule to impede common health care practices (e.g., hospitals discussing treatment options with spouses and relatives, and family members picking up a prescription).

Does the Rule Restrict Parental Involvement and Notification? In general, a parent is deemed to have the rights associated with a minor's health information, including the right to authorize disclosure or to request access to the information. But if a minor is authorized by law to consent to treatment and has consented to care (with or without the consent of a parent), or if the parent has assented to an agreement of confidentiality between a provider and a minor, then the minor has the exclusive rights associated with that information. The rule, however, defers to state parental notification laws. It allows covered entities to disclose a minor's information to a parent (or provide the parent with access to such information) if such disclosure is permitted or required by state law. Similarly, disclosure to (and access by) a parent is prohibited where prohibited by state law. Where state law is silent or unclear about

parental notification, the rule permits a covered entity to provide or deny access to the parent provided that action is consistent with state law.

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: disclosures to or requests by a provider for treatment purposes; disclosures made to patients upon their request; disclosures made to the Secretary to enforce compliance; authorized uses or disclosures; 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 under the privacy rule 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? Health plans and health care providers must provide patients with a written notice of their privacy practices. Plans are required to give notice at enrollment. 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.

Can Health Information Be Used for Marketing? A covered entity may not disclose health information to a third party (e.g., pharmaceutical company), in exchange for direct or indirect remuneration, for the marketing activities of the third party without first obtaining a patient's authorization. Similarly, a covered entity may not use or disclose health information for its own marketing activities without authorization. However, communications made by a covered entity (or its business associate) to encourage a patient to purchase or use a *health care-related product or service* are not defined as marketing under the rule and, therefore, do not require the patient's authorization, even if the covered entity is paid. Such communications include

prescription refill reminders and information about alternative treatments, as well as more controversial activities paid for by third parties (e.g., communications by pharmacies, paid for by a drug manufacturer, that recommend patients switch their medication to the company's product).

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 unless they take reasonable steps to correct the problem and, if such steps are unsuccessful, terminate the contract or report the problem to HHS.

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.

How Will the Rule Be Enforced? Any person who believes a covered entity is not complying with the privacy rule may file a complaint with HHS's Office of Civil Rights (OCR), which is responsible for implementing and enforcing the rule. OCR is working with covered entities to encourage voluntary compliance. It says that enforcement of the rule will be reactive and complaint-driven. Under HIPAA, OCR has the authority to impose civil monetary penalties against covered entities that fail to comply with the rule, and the Department of Justice may seek 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 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. HIPAA did not provide a private right of action for individuals to sue for violations of their health information privacy in federal court. However, nothing in HIPAA prohibits aggrieved individuals from filing a state law claim against a covered entity for its noncompliance and resulting harm.

Where Can I Obtain More Information? General information on all the HIPAA standards can be found at [http://aspe.os.dhhs.gov/admnsimp]. Implementation guidance, answers to frequently asked questions, and other details on complying with the privacy rule may be found on the OCR website at [http://www.hhs.gov/ocr/hipaa].