Order Code RS20500
Updated September 10, 2001

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 (65 Fed. Reg. 82462) to protect the privacy of personally identifiable medical information. The rule covers health care providers, health plans, and clearinghouses (i.e., entities that facilitate and process the flow of information between providers and payers). Under the rule, patients have the right to inspect and amend their medical records. Providers are required to obtain a patient's one-time, written consent to use or disclose health information for routine health care operations (e.g., treatment and payment). In addition, health plans and providers must get a patient's specific authorization to use or disclose information for non-routine uses and most non-health care 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 rule took effect on April 14, 2001, and most covered entities have 2 years to comply. On July 6, 2001, HHS issued the first of several guidance documents to accompany the rule. The guidance clarifies the rule's provisions and reiterates the department's intent not to interfere with patients' access to health care or the quality of health care delivery.

Introduction

On December 28, 2000, the Secretary of Health and Human Services (HHS) issued a comprehensive health privacy regulation to protect medical records and other personal health information maintained by health care providers, health plans, and health care clearinghouses. The health privacy rule gives patients the right to access and amend their medical records, limits the use and disclosure of personal health information without a patient's written consent, requires health plans and health care providers to notify patients about the use and disclosure of their medical information, restricts most disclosure 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 billing and other common transactions, 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 on November 3, 1999, based on principles outlined in a September 1997 report to Congress.[1] HHS reviewed more than 52,000 public comments on its proposed rule before publishing the final rule on December 28, 2000. The rule took effect on April 14, 2001. Covered entities have 2 years, or until April 14, 2003, to comply with the rule. Small health plans with annual receipts of $5 million or less have an additional year to comply.

Questions and Answers About The Health Privacy Rule

Who Is Covered? Under HIPAA, the Secretary only has the authority to regulate health care providers who conduct certain financial and administrative transactions (e.g., billing) electronically, health plans, and health care clearinghouses. These three groups are defined as covered entities. The regulation, therefore, does not directly apply 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, the rule requires covered entities to sign contracts with their business associates that would essentially bind those associates to the covered entities' privacy practices. Business associates are defined as those who receive health information from a covered entity, as well as those who receive or create health information on behalf of a covered entity (e.g., lawyers, auditors, consultants, billing firms, benefit managers).

---

[1] The report is available online at [http://aspe.os.dhhs.gov/admnsimp/pvcrec.htm].

What Type Of Health Information Is Covered? The rule covers all personally identifiable health information created or received by a covered entity, including paper records, electronic records, and oral communications. Non-identifiable health data, from which all personal identifiers have been removed, are not subject to the rule.

Can Patients Access Their Health Information? Yes, the rule requires health plans and health care providers to allow patients to see and copy their health information. Covered entities are permitted to charge a reasonable, cost-based copying fee. Patients may also request amendment or correction of health information that is incorrect or incomplete. Finally, patients have a right to receive a history of disclosures of their health information, except to carry out routine health care operations (e.g., treatment, payment).

Does Use And Disclosure Of Health Information Require Patient Consent? Yes, health care providers *must* obtain a patient's one-time consent in writing before using or disclosing personally identifiable health information for treatment, payment, and other routine health care operations (e.g., quality assessment, performance review, training programs, licensing, audits). Providers *may* condition treatment on obtaining such consent. Consent is optional for providers who have an indirect relationship with patients (i.e., they have no direct contact with patients, or they provide services at the request of another provider). Health plans and health care clearinghouses *may* also obtain a patient's consent for their own use or disclosure of health information to carry out these three core health care functions, and *may* condition enrollment on obtaining such consent. Patients have the right to request that covered entities restrict the use and disclosure of their health information for payment, treatment, and health care operations. However, covered entities are not required to agree to such a request. Patients may revoke their consent at any time.

In addition, covered entities *must* obtain a patient's specific authorization in writing before using or disclosing health information for non-routine uses and most non-health care purposes; for example, releasing information to financial institutions that offer mortgages and other types of loans, or selling mailing lists to marketing companies. In general, health plans and health care providers cannot condition treatment, payment, or enrollment on receiving a patient's authorization to disclose health information for non-routine uses. Patients may revoke their authorization at any time.

Can Health Information Be Used Or Disclosed Without A Patient's Authorization? Yes, the rule 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:

Public Health Activities. Disclosures may be made for public health purposes (e.g., reporting diseases, collecting vital statistics), as required by state and federal law.

Health Oversight. Health information may be disclosed to public agencies to conduct activities such as audits; inspections; civil, criminal, or administrative proceedings; and other activities necessary for oversight of the health care system.

Law Enforcement. 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 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).

Judicial and Administrative Proceedings. Protected information may be disclosed in judicial and administrative proceedings if the request for the information is made through or pursuant to a court order.

Research. Covered entities may use or disclose health information for research without a patient's authorization, provided an Institutional Review Board (IRB) or privacy board reviews the research protocol and waives the patient consent 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 organ and tissue procurement 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.

Does The Rule Restrict Employers' Access To Health Information? Yes, employers that sponsor health plans may not obtain and use employees' health information for purposes unrelated to providing and paying for health care (e.g., hiring and promotion decisions) without their specific authorization.

Does The Rule Permit Marketing And Fundraising By Covered Entities? Yes, covered entities may use or disclose a patient's health information to prescribe, recommend, or sell their own products and services, or the products and services of others, as part of the treatment of that individual. They must identify themselves when making a marketing appeal and give patients the opportunity to opt out of receiving any further communications. Covered entities are also permitted to disclose certain patient information to a foundation or business associate that contacts patients for fundraising purposes, provided the patients are given the opportunity to opt out of any further communications.

Are Plans and Providers 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, including a description of the patients' right to inspect and copy their health information and a list of the anticipated uses and disclosures of that information that may be made without patients' authorization. Plans and providers are required to update the notice as necessary to reflect changes in their privacy practices and to adhere to the practices specified in the most current notice.

---

[2] Federally funded research involving human subjects, and clinical trials of new drugs and medical devices, are subject to a set of federal regulations called the Common Rule. Under the Common Rule, the research 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. The health privacy rule would require all research involving human subjects, regardless of its source of funding, to undergo review by an IRB or an equivalent, newly formed privacy board.

Are There Limits On The Amount Of Information Disclosed? The rule requires covered entities to disclose no more than the minimum amount of personally identifiable health information necessary to accomplish the intended purpose of the disclosure. However, treatment-related disclosures to and requests by health care providers are not subject to the minimum necessary standard.

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 obtaining such authorization.

What Must Covered Entities Do To Ensure Compliance? Covered entities must develop and implement various administrative procedures, commensurate with the size and scope of their business, to safeguard 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, but they may be held responsible if they know of a violation and fail to take reasonable steps to correct the problem.

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. The Secretary was constrained under HIPAA from giving individuals the right to sue for violations of the law.

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. Several states permit competent minors to obtain medical treatment without a parent's consent. State laws that authorize or prohibit disclosure of a minor's health information to a parent are not preempted by the privacy rule.

How Much Will It Cost To Implement The Rule? HHS estimates that implementing the privacy regulation will cost $17.6 billion over 10 years. According to the agency, this amount will be more than offset by the 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 $12.3 billion in improved health care efficiency and privacy protection.[3]

Is HHS Providing Guidance And Planning To Modify The Rule? On July 6, 2001, HHS issued the first of several guidance documents to clarify key provisions of the rule and address industry concerns that the rule will compromise patient care by placing unacceptable restrictions on access to health information and be extremely costly to implement. Hospitals, health insurers, and pharmaceutical companies are especially critical of the rule's general consent requirement, the minimum necessary standard, and the business associate contracts. The guidance reiterates the agency's intent not to interfere with patients' access to health care or adversely impact the quality of care. HHS also intends to modify some of the rule's provisions. HIPAA gave the Secretary the authority to modify the rule after it takes effect in order to permit compliance. However, any significant modifications to the rule would require the agency to reopen the rulemaking process by publishing a Notice of Proposed Rulemaking and providing for public comment before issuing a revised final rule.

Patient privacy advocates strongly support the rule, though they too have concerns. 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. Consumer advocates have urged HHS not to weaken any of the rule's privacy protections.

Would Legislation To Delay HIPAA's Administrative Simplification Standards Impact The Privacy Rule? Lawmakers have introduced legislation that is intended to delay implementation of all the HIPAA standards except the privacy rule (i.e., transactions and codes, security, unique identifiers). S. 836 and H.R. 1975 would set October 16, 2004 as the uniform compliance date, or 24 months after all the standards are published, whichever is later. Although neither bill directly covers the privacy rule, it is unclear whether the rule would be impacted. Under HIPAA's general applicability provisions, the privacy rule applies to providers who conduct any of the HIPAA-specified health care transactions electronically. Some analysts claim that without transactions standards in effect, the privacy rule would not apply to providers.

Where Can I Obtain More Information? Information on the HIPAA standards, including the text of all the *Federal Register* notices, summaries of the proposed and final regulations, public comments, and the HHS implementation plan can be found on the agency's Administrative Simplification Web page [http://aspe.os.dhhs.gov/admnsimp]. HHS's Office of Civil Rights, which is responsible for implementing and enforcing the privacy rule and is responding to questions about the rule, has established a privacy home page [http://www.hhs.gov/ocr/hipaa]. For more analysis of the health privacy rule and the accompanying guidance, see CRS Report RL30620: *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations.*

---

[3] HHS issued the electronic transactions and code sets rule on August 11, 2000 (65 Fed. Reg. 50311). The rule establishes standard electronic formats and data content for claims and other common health care transactions.