

Patient Information Privacy: HIPAA Provisions and Patient Safety Issues

Bryan A. Liang MD, PhD, JD

The privacy of patient health care information is an important issue. Inappropriate use of private, patient-identifiable information has resulted in significant federal legislation attempting to address this growing concern. The major federal statute in this area is the Health Insurance Portability and Accountability Act (HIPAA), passed in 1996.¹ The statute required that federal privacy legislation be enacted by Congress by August 21, 1999, with the default—in the event of congressional inaction—being the Secretary of the Department of Health and Human Services (DHHS) issuing proposed privacy rules. Congress did miss its own deadline, and thus DHHS issued proposed regulations for privacy in 1999; final regulations were issued late in 2000. For large health plans, the deadline for full implementation of these regulations is February 26, 2003; small health plans (but not other small businesses) have a full 36 months to comply with them. Since these regulations cover virtually every health care provider and virtually all health care information, physicians and other providers must be cognizant of their provisions to avoid the significant penalties associated with the rules.

HIPAA PROVISIONS

Coverage

HIPAA covers all identifiable patient health care information in any form—oral, written, or electronic—maintained or transmitted by a wide array of “covered entities,”² including providers, health care clearinghouses, contractors, subcontractors, and health plans.³ These entities must (1) designate a privacy official or contact person to address complaints and provide privacy information; (2) develop employee privacy training programs; (3) implement “appropriate” administrative, technical, and physical safeguards against unauthorized access and mistaken misuse; (4) create a mechanism of complaint for the entity’s privacy practices; and (5) develop employee sanctions for violations of the rule and covered entity’s privacy policies.⁴

In addition, business associates of all of these entities are subject to the HIPAA privacy regulations, including those who provide legal, actuarial, accounting, consulting, management, accreditation, data aggregation, and financial services, as is any other entity that receives protected health information from or performs a function or activity on behalf of the covered entity.⁵ Contracts between the parties must limit business associate use and disclosure of patient information to parties specified and must require particular security, inspection, and reporting mechanisms by the business associates as well as subcontractors used by the business associates. Internal records must be made available to the Secretary of the DHHS, and all protected information must be returned or destroyed at the end of the contract period, if practical.⁶ The health care entity may be held responsible for rule violations of its business associates if it has knowledge of them.⁷

Patients have the right to inspect their health care information, copy and amend it, authorize (or forbid) its use, and receive formal accounting of how their information is used.⁸ When patients request access, copying, inspection, and amendments of their medical records, covered entities have time limits to respond to these requests.⁹ Infrastructural component barriers (eg, firewalls, electronic buffers) must be used to block unauthorized access to medical data in electronic format.¹⁰

Case Presentation

An internal medicine resident at a community hospital sees a 66-year-old woman with stage IV large cell lymphoma who has been admitted for chemotherapy and management of her chronic pain.

HIPAA issue. In accordance with HIPAA regulations, the physician must obtain written HIPAA consent from

Dr. Liang is a Professor of Health Law and Policy, Health Law and Policy Institute, University of Houston Law Center, Houston, TX; and a member of the Hospital Physician Editorial Board.

the patient for access to her medical records for treatment, payment, and other standard health care functions (eg, insurance eligibility determination) if he or the hospital has not done so already.

Consent, Authorization, and Exceptions

Definitions. Written patient HIPAA consent for use of identifiable patient information is required for routine treatment, payment, and health care operations¹¹; all other uses generally require specific and detailed written HIPAA authorization. Both consent and authorization can be revoked at any time.¹² Patient treatment cannot be predicated on whether the patient consents to the disclosure unless he or she refuses to allow information disclosure for treatment or enrollment determinations at the time of enrollment. Authorizations also cannot be predicated on patient agreement and must be voluntary and specific as to the information to be disclosed.¹³

There are, however, exceptions to the patient consent and authorization requirements.¹⁴ Exceptions to consent include situations in which a serious threat to health or safety must be averted, circumstances in which treatment is legally required, and situations in which there are substantial barriers to communicating with the patient (eg, mental incompetence).¹⁵

Exceptions to authorization requirements include use for health oversight activities, public health activities, and research. Additionally, law enforcement, legal proceedings, marketing, public safety and welfare circumstances, and listing in facility patient directories require no or limited patient approval.¹⁶

It is important to note, however, that the use and disclosure of patient information must be performed under the restrictions and requirements of the HIPAA rules. Indeed, an entity cannot use or disclose information in any other forum, even if legal as defined by the rule, if patient approval is given only for limited use or the covered entity has agreed to a particular limitation.¹⁷

Continuation of case. Once the physician has obtained or verified that the patient has provided HIPAA consent, he may begin reviewing her medical records to plan her treatment regimen. The physician writes the relevant orders for chemotherapy and pain medications for the patient's inpatient stay. A day after writing the order, he visits the case patient during rounds. When he arrives at her room, he notes that the assigned nurse is about to administer an antibiotic agent through the patient's intravenous line. The physician prevents this action and then discusses with the nurse the conflict between his order and the material to be

infused. The nurse rechecks the order sheet in the chart, which does have the correct drug indicated. However, the nursing medication notes have incorrectly indicated that the patient is to receive the antibiotic intravenously (the drug appears intended for the patient's roommate). The physician realizes that this is a "near miss" error and thus may be indicative of important systems issues. He desires to assess all patients in the facility who might be or have been subject to medication errors because of a conflict between nursing and chart medication orders.

HIPAA issue. If the physician wishes to assess medical records of all patients who required medication and may have been subject to a medication error, he is subject to the HIPAA medical privacy provisions. He will not be able to access these patient records under standard consent, because such safety activities and research do not fall within the consent provisions. He also will not be able to access patient records on the basis of any HIPAA consent exceptions. His efforts do not fall within specified marketing, lawsuit, law enforcement, or other uses noted in the regulations.

The physician may be able to access patient records under patient authorization. However, the extensive requirements to be fulfilled (ie, detailed descriptions of the exact information desired, the requisite legal form of the request, the exact use of the information, the specific person or persons who will have access to the information), as well as other stipulations, will be difficult for him to meet and for patients to understand. Furthermore, because the physician is attempting to engage in qualitative patient safety work, it will be difficult to determine before reviewing the records what kinds of medications were taken and what characteristics about the patient (eg, his or her hospital stay, social situation, previous hospital stays, previous hospital diagnoses, other potentially useful systems factors) may need to be assessed, as well as the kinds of cultural issues that may contribute to potential medication errors at the facility.

Continuation of case. The physician notes that he cannot perform the safety analyses he desires under HIPAA consent, under consent exceptions, or, practically speaking, under HIPAA authorization. He thus attempts to obtain permission to analyze potential medication errors he has noted under the authorization exception of research.

HIPAA issue. The physician requests that the hospital's institutional review board (IRB) review his proposed project. However, the IRB indicates that it does not currently have guidance to determine how to ensure medical privacy of patient records under the

current HIPAA regulations, because no guidance is provided. Furthermore, the IRB notes that a privacy board might be a more suitable body to determine the acceptability of the physician's proposed project. However, because the hospital does not yet have a privacy board and does not know how it should appropriately function and because the HIPAA regulations do not provide guidance in this area either, the IRB indicates that it may not be able to approve the physician's project.

Continuation of case. After consulting the IRB, the physician assesses secondary sources on the HIPAA medical privacy rules and notes that he may be able to perform his safety project under the research safe harbor of deidentification. He proposes to the IRB that he will deidentify records and then review conflicts between chart orders and nursing medication notes.

HIPAA issue. The IRB indicates that because the facility is a small community hospital, it must be very concerned about the potential for identification of the patient from its records. The board notes that, for example, because there are not many patients with stage IV large cell lymphoma in the community, the case patient's identity would be clear on the basis of diagnosis if the physician were to access her records. Furthermore, other inpatients who may have been subject to an actual medication error may be known because of the error itself or may be identified by their diagnoses. The IRB thus decides to reject the physician's efforts to obtain this information.

"Minimum Necessary" Standard

Health care providers should also note that when disclosure and use of medical information is allowed with or without patient authorization, the covered entity must have policies and procedures in place that generally limit disclosure to the "minimum necessary" information, with limited exception for treatment-related disclosures to providers by covered entities. This standard requires that only the information necessary to accomplish the purpose for which the information is used or disclosed be released, taking into consideration practical and technologic considerations and costs.¹⁸

Penalties

To ensure a strong incentive to err on the side of too little disclosure of information rather than too much, violation of the HIPAA rules imposes civil monetary penalties up to \$25,000 for each standard violation as well as criminal penalties of imprisonment of up to 10 years and a fine of up to \$250,000.¹⁹ Criminal sanc-

tions and civil penalties can be levied for the same violation.²⁰ The federal law represents a floor of protection for medical privacy; stricter state laws are not preempted.²¹ Many other federal statutes may interact with these privacy provisions.²² Thus, providers who are deemed to violate HIPAA provisions may also be penalized under other state and federal laws.

PROBLEMS FOR PATIENT SAFETY

Although patient privacy is an important goal, many of the provisions under HIPAA may have a negative impact on quality efforts, particularly patient safety activities. Because of the extensive costs associated with compliance and the relatively voluntary status of patient safety activities, the medical privacy provisions may force providers into an uncomfortable position of fulfilling compliance-based rules under HIPAA to the exclusion of quality efforts in reducing medical errors and promoting patient safety.²³

Indeed, the very entities that must investigate and implement safety and safety advances are those in the community setting, both nonurban and rural environments. The Health Care Financing Administration (now the Centers for Medicare and Medicaid Services) reports that between 80%²⁴ and 85%²⁵ of all health care entities shouldering the costs for the privacy rule are small businesses, which represent more than 560,000 organizations in the United States. Small business providers include community and rural health plans, hospitals, nursing facilities, physicians, pharmacies, laboratories, durable medical equipment suppliers, billing companies, companies that sell health care software, and others.

Consequently, the percentage of community providers on the health delivery front lines that are small businesses is high: approximately 90% to 97% of all physician offices and clinics and 50% of all hospitals fall within this category. Furthermore, the fraction of nonurban community providers that are small businesses and do not have extramural funding to offset at least some of the costs for safety work are even higher. These providers are significantly vulnerable to any increases in costs because they have traditionally suffered negative operating margins, compared with their urban and academic counterparts.²⁶ Additionally, these small business health care providers, although they represent the vast majority of entities covered by the rule, only receive "but a small portion of the revenue stream . . . 30.2% of the total [healthcare revenues]."²⁷ Therefore, not only does the privacy rule affect the vast majority of health care providers, it may disproportionately impose the costs of compliance on these community providers relative to

their health care income and receipts. This reality may force these providers into making an uncomfortable choice between privacy and safety. Providers must therefore carefully assess the effects of short- and long-term allocation of resources and focus on determining how to make difficult decisions regarding patient safety and privacy.

CONCLUSION

Patient information privacy is an important concern, and federal legislation has been adopted in an effort to ensure it. All providers will be affected by this rule, and adherence to its provisions is necessary to avoid the significant legal penalties associated with violations. Although privacy is important, in their current iteration, the medical privacy provisions may impede significant patient safety work and progress. Providers should carefully consider how to fulfill both of these important goals so that they can best serve the interests of their patients.

UPDATE

Recently, the federal government has proposed limiting the HIPAA consent provisions. As of July 2002, these provisions have not yet been finalized. **HP**

REFERENCES

1. Pub L No. 104-191.
2. 45 C.F.R. Sect. 164.500, 164.501.
3. 45 C.F.R. Sect. 160.103, 160.105, 164.500.
4. 45 C.F.R. Sect. 164.530.
5. 45 C.F.R. Sect. 160.103, 164.502, 164.504.
6. 45 C.F.R. Sect. 164.504(c), 164.504(e).
7. Final rule: Standards for privacy of individually identifiable health information. 65 Federal Register 82461-82829:82476 (2000).
8. 45 C.F.R. Sect. 164.524, 164.526, 164.528.
9. 45 C.F.R. Sect. 164.524, 164.526.
10. 45 C.F.R. Sect. 164.504(c).
11. 45 C.F.R. Sect. 164.506.
12. 45 C.F.R. Sect. 164.506, 164.508.
13. 45 C.F.R. Sect. 164.506(b).
14. 45 C.F.R. Sect. 164.512.
15. 45 C.F.R. Sect. 164.506(a), 164.512(j).
16. 45 C.F.R. Sect. 164.510, 164.512(f).
17. 45 C.F.R. Sect. 164.522.
18. 45 C.F.R. Sect. 164.502, 164.514(d).
19. Pub L No. 104-191, Sect 262.
20. Liang BA. Concepts of law. In: Health law and policy: a survival guide to medicolegal issues for practitioners. Boston: Butterworth-Heinemann; 2000.
21. 45 C.F.R. Sect. 160.201, 164.202, 164.203.
22. Final rule: Standards for privacy of individually identifiable health information. 65 Federal Register 82461-82829:82482-82487 (2000).
23. Liang BA. The adverse event of unaddressed medical error. *J Law Med Ethics* 2002. In press.
24. Final rule: Standards for privacy of individually identifiable health information. 65 Federal Register 82461-82829 (2000).
25. Proposed rule: Standards for privacy of individually identifiable health information. 64 Federal Register 59917-60065.
26. Mohr PE, Blanchfield BB, Cheng CM, et al. The financial dependence of rural hospitals on outpatient revenue: working paper. Bethesda (MD): Project HOPE Walsh Center for Rural Health Analysis; 1998.

Copyright 2002 by Turner White Communications Inc., Wayne, PA. All rights reserved.