2003

HIPAA Regulations: A New Era of Medical-Record Privacy?

George J. Annas

LEGAL ISSUES IN MEDICINE

HIPAA Regulations — A New Era of Medical-Record Privacy?

George J. Annas, J.D., M.P.H.

Although the regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regarding the privacy of medical records are new,[1] the concept of using federal law to protect the privacy of medical records is not. The substance of the new regulations can be traced back to work done in the 1970s, especially the report of the Privacy Protection Study Commission, which helped to articulate the case for national privacy standards for a variety of records kept on citizens.[2] The Clinton Health Security Act contains a separate section entitled "Privacy of Information" that sets forth the framework for the national standards created by the HIPAA regulations.[3] Provisions for the privacy of medical records became part of HIPAA,[4] which authorized the secretary of Health and Human Services to promulgate regulations to protect the privacy of health information in which the patient is identifiable in the event that Congress did not enact legislation on this subject (which it did not).

In the context of the Clinton health plan, rules for the privacy of medical records were part of a much broader package whose main aim was to provide access to health insurance for all Americans. Now regulations for medical-record privacy have arrived alone. I believe the new regulations are excessively and unnecessarily complex and often more attuned to making sure that businesses and government agencies get access to medical records than to the protection of patients' privacy. The debate over the content and effect of the HIPAA regulations has been fierce over the past four years and is likely to intensify in the post–September 11 era of surveillance, which has brought even more proposals to authorize virtually unlimited access to medical records by national security, law-enforcement, and public health agencies.[5-7]

A new cadre of HIPAA consultants has grown up in the past few years, and hospitals, health plans, and many physician-run practices have found their help essential in understanding how to comply with the new regulations. This need arises because although the core principles behind the regulations are readily understandable, the regulations themselves are long, complex, and overlaid with commentary. Moreover, we have been through three different versions of the "final" regulations in the past two years, and there will undoubtedly be more changes as they are implemented.

My purpose in this article is not to provide an in-depth analysis or critique (the regulations are filled with compromises, and few people are entirely happy with them), but rather to provide a basic summary aimed primarily at the practicing physician. Whatever one's view of the HIPAA regulations, they will form the starting point for future national regulation of medical privacy. In this sense, they are akin to movie contracts, about which one Hollywood executive is reported to have said, "We have to have a contract so we have a basis for renegotiation."

PRINCIPLES OF PRIVACY

It has been foundational, at least since Hippocrates, that patients have a right to have personal medical information kept private. Physicians have an obligation to keep medical information secret. The chief public-policy rationale is that patients are unlikely to disclose intimate details that are necessary for their proper medical care to their physicians unless they trust their physicians to keep that information secret. Basic privacy doctrine in the context of medical care holds that no one should have access to private health care information without the patient's authorization and that the patient should have access to records containing his or her own information, be able to obtain a copy of the records, and have the opportunity to correct mistakes in them.[8]

The HIPAA regulations can be seen as an overly complicated way of applying these basic privacy rules in an era of electronic communication, large health plans, and fierce marketing campaigns. Compliance is required by April 14, 2003, and the regulations apply to both electronic and paper records. A physician is covered by the regulations (be-

comes a "covered entity," in the language of the regulations) if he or she conducts any medical business, including billing, electronically, even if the physician contracts with another entity or business associate to do billing. This means that most practicing physicians will be covered, since most physicians accept private health insurance, are members of one or more health plans, receive payment from Medicare or Medicaid, or otherwise do business electronically.

All of the HIPAA rules include an implicit requirement that the amount of individually identifiable health information released or requested for any specific purpose — except for disclosures authorized by the patient, disclosures to another health care provider involved in treatment, or disclosures required by law — be the "minimum necessary" to accomplish the purpose. This means that outside the context of treatment, a patient's entire medical record can seldom be lawfully disclosed without the patient's written authorization.

The HIPAA regulations set a federal minimum, or floor, not a ceiling, on the protection of privacy. Thus, when other federal laws (such as laws protecting drug and alcohol treatment records) or state laws (such as laws that provide special protections for mental health or genetic records) provide more protection for patients' privacy than the new regulations, the more protective federal and state laws will continue to govern. In addition, state law continues to govern parent–child relationships, the rights of children, and the definitions of emancipated and mature minors. Federal regulations cannot change a state's family law or its informed-consent laws, even if the Department of Health and Human Services wanted to do so. Of course, the continued importance of state law means that the regulations ultimately fail to produce a real national standard of medical privacy — because the application of the regulations can and will vary from state to state.

THE PRIVACY NOTICE

Few Americans have any idea what is done with their medical records, and probably fewer still believe they can have any control at all over who uses them. There are certainly computer experts who share the view that personal control of private information is an illusion in the computer age and that privacy is already dead. The HIPAA regulations reject this view and instead aim to inform and educate patients about their privacy rights. That is why all patients must be provided with a privacy notice. The regulations require that each patient be provided with a written "notice of privacy practices" on the day of the first delivery of health services after the regulations become effective and that the notice itself be prominently posted at the service site.

The privacy notice must tell the patient who will be able to see and use the patient's medical records, what uses will require the patient's specific authorization, and that patients have the right to inspect, copy, and amend their medical records and to obtain an accounting of disclosures. The notice must also contain the name, title, and telephone number of a person or office to contact, usually designated as a privacy officer (this person could be the physician's office manager, for example), for further information. A good-faith effort must also be made to obtain the patient's written acknowledgment of receipt of the notice. Most notably, and contrary to an earlier proposal that the patient's consent be required for all uses of the medical record, patients are simply informed in this notice that their medical records can be disclosed for uses related to treatment, payment, or "health care operations" without any additional notification or authorization. At least one example of each of these uses must also be provided in the notice.

Treatment-related uses of the medical record have always been a reasonable expectation on the part of both physicians and patients, although people have been genuinely surprised to learn how many members of a hospital staff have routine access to their medical records.[8,9] Use of medical records for payment-related purposes has historically required patients' authorization, but this usually involved the simple signing of a form in the waiting room, and refusal to sign meant that a patient had to pay out of pocket, so there has never been any real choice in this matter. "Health care operations," as defined in the regulations, is a much broader category and includes such uses as quality assessment (other than research), performance evaluation, the conduct of training programs, the rating of premiums, auditing, business planning, and management. This is a compromise. Privacy advocates generally favor the earlier version of the rule that required consent for all uses of the medical record, including treatment.[10] Under the new rule, providers can still obtain consent, but why would a provider do so if a notice alone is sufficient? On the other hand, since even the earlier rule permitted

physicians to require that the patient consent to the use of the medical record for these purposes as a condition of treatment, voluntary consent was never really required.

AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

Under the terms of HIPAA, a valid authorization to release health information must contain at least the following: "a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion"; "the name [of the person or entity] authorized to make the use or disclosure"; "the name [of the person or entity] to whom the disclosure may be made"; "a description of each purpose of the requested use or disclosure"; "an expiration date or expiration event" ("none" or "end of the research study" is sufficient for research-related use, research data bases, or research repositories); and "the signature of the individual and date."[1]

The authorization form must be in plain language; a copy must be provided to the patient; and the form must include a notice of the patient's right to revoke the authorization, the effect on the patient's benefits of not signing, and the potential that the information will be disclosed to unauthorized persons by the receiver. Thus, authorization to release medical-record forms can no longer contain blanks for the persons or entities who are to be provided with information about the patient, for the information to be provided, or for the expiration date; such incomplete authorizations are "defective" and invalid under the new regulations.

PATIENTS' RIGHTS TO MEDICAL RECORDS

Under the regulations, patients have the right to inspect and obtain a copy of their entire medical record, with the exception of notes from psychotherapy (notes of a mental health professional that document or analyze "the contents of conversation during a private counseling session . . . and are separated from the rest of the individual's medical record") and "information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding."[1]

There are three very narrow grounds on which physicians can refuse to make the entire medical record available to the patient. The patient has the right to have a refusal reviewed by another licensed health care professional (other than anyone who participated in the decision to deny access) designated by the refusing entity, and the entity must provide access to the medical record if the reviewer determines that it should do so. Access may be refused if "a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person"; if "the protected health information makes reference to another person [and] the access requested is reasonably likely to cause substantial harm to such person"; or if "the request for access is made by the individual's personal representative [and access by that person] is reasonably likely to cause substantial harm to the individual or another person."[1]

A reasonable, cost-based fee can be charged for copying, including the labor costs of copying, and postage, if applicable. Persons may also request amendments to their medical records. Physicians can require requests for amendments to be in writing and to state the reason for the requested amendment. Amendment can be denied if the person or entity to whom the request is made did not create the information or if the information is deemed to be accurate and complete. When an amendment is made, at the minimum, the amendment must be appended or linked to the record it is amending, and reasonable efforts must be made to inform others who have been provided with the original information about the amendment. If amendment is denied, the person has the right to have a statement of disagreement (to which the entity may respond as well) appended to the disputed medical record.[1]

A person also has the right to an accounting of disclosures of protected health information made over the previous six years. There are, however, numerous exceptions to this accounting requirement, including disclosures for use in treatment, payment, and health care operations, disclosures authorized by the person or required by law, disclosures for use in a facility directory or for national security or intelligence purposes, or disclosures that occurred before the compliance date for the new regulations.[1] The accounting must include the date of disclosure, the name and address of the person or entity who received the information, and a brief description of the information disclosed and the purpose for which it was disclosed.

CHILDREN, EMERGENCIES, AND RESIDENT TRAINING

Three examples help to illustrate how the HIPAA rules apply and how they relate to other laws. The first deals with minors. As noted above, state law defines the legal rights of children and their parents, and state law continues to govern parental rights to access to a child's medical record. Under the regulations, parents have a right to have access to the medical records of their minor children as long as parental access is consistent with state law. Parents are the personal representatives of their children under the regulations unless it is the minor who lawfully consents to treatment, the minor obtains care at the direction of a court or a person appointed by the court, or the parent has agreed in advance with the health care provider that the relationship between the child and the health care provider will be confidential. The final grounds for refusal of access to medical records, regarding a request by a personal representative, apply to children as well: a physician can deny parents access to their child's medical records if the physician reasonably believes that access is likely to cause "substantial harm," such as physical violence by the parent against the child.

Rules and procedures for emergency treatment are not affected by the privacy regulations, and generally the regulations mirror common sense in this context. Emergency care providers, for example, are not required to provide patients with a privacy notice at the time of rendering emergency care (the rule in a medical emergency, "treat first and ask legal questions later," still applies).[8] Nonetheless, after the emergency has ended, the regulations require that patients be provided with a privacy notice, although in this instance, the regulations do not require documentation of a good-faith effort to obtain the patient's written acknowledgment of receipt of the notice.

The question of whether medical students and house officers can have access to entire medical records is addressed by the definition of health care operations (activities that do not require specific authorization by the patient for access to records) and the application of the requirement that the amount of information disclosed be the "minimum necessary." The regulations specifically include "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers" as part of the definition of health care operations.[1] The "minimum necessary" rule, as noted above, itself has exceptions, and does not apply to anyone involved in the treatment of the patient. Moreover, the Office for Civil Rights of the Department of Health and Human Services, the office charged with interpreting and enforcing the regulations, has suggested that hospitals "can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients' medical information, including entire medical records."[11]

MEDICAL RESEARCH

The new regulations have greatly simplified what were highly contested provisions.[12,13] Nonetheless, critics continue to believe that even the simplified research regulations will discourage entities from making medical records available for research and will diminish "the pace and volume of research."[14] I think this assessment is overly alarmist. On the other hand, it is a bit strange to see the federal government focusing so much attention on protecting the medical records and privacy of human subjects when it is the autonomy, health, and safety of human subjects that need and deserve greater protection in the research setting.[15]

Although they are similar to the "common rule" that governs research using human subjects,[16] the HIPAA regulations apply to all medical research regardless of its source of funding. To oversimplify a bit, medical records can be used for research without the authorization of the subject if the records are "de-identified" (so that the records cannot be easily linked to a specific person), if they are part of a "limited data set" (in which data are stripped of most, but not all, identifiers, and the recipient or research entity signs an agreement consenting to adhere to specific limitations on use and not to identify or contact the subjects), or if the institutional review board (or a new privacy board) permits a "waiver" of consent under specific rules. Research-specific regulations have also been added to the latest version of the HIPAA regulations. For example, the right of a patient to gain access to medical records can be temporarily suspended as long as medical research that includes treatment is in progress, at least if this condition was agreed to by the patient at the time he or she consented to be a research subject and if he or she was informed that the right to access would be reinstated on completion of the research trial. Neg-

ative reactions to the HIPAA regulations regarding the use of medical records in research are at least partly the result of the fact that there is currently no national standard for providing researchers access to medical records. Practice varies widely among institutions and among institutional review boards. Unfortunately, to the extent that local institutional review boards retain the discretionary authority to grant waivers of consent, a national standard for the use of medical records in research may not develop.

ENFORCEMENT

Enforcement of the regulations is in the hands of the Office of Civil Rights. The secretary of Health and Human Services has the authority to impose a civil money penalty of not more than $100 for each violation, not to exceed $25,000 annually for violations of the same requirement.[17] The possibility of criminal penalties has been used to frighten physicians, although it seems highly unlikely that any physician would ever act in such a way as to be subject to them. Specifically, HIPPA permits persons who knowingly "obtain" or "disclose" individually identifiable health information to be fined not more than $50,000 and imprisoned for not more than 1 year (the limits are $100,000 and 5 years if the crime is committed under false pretenses, and $250,000 and 10 years "if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm").[18]

CONCLUSIONS

The implementation of the new HIPAA privacy regulations is likely to be costly, inconsistent, and frustrating to both physicians and patients. Medical privacy is critical to most Americans, national privacy standards would be welcome, and the promise of privacy remains essential for much medical treatment. Nonetheless, the new privacy rules are primarily procedural in nature, are incapable of setting a national privacy standard, and are being imposed by fear rather than agreement on principles. Medical privacy deserves protection but should be seen as part of health care and not as an end in itself.

From the Health Law Department, Boston University School of Public Health, Boston.

1. Office of Civil Rights, Department of Health and Human Services. Standards for privacy of individually identifiable health information: final rules. Fed Regist 2002;67(157):53182-272.
2. Privacy Protection Study Commission. Personal privacy in an information society. Washington, D.C.: Government Printing Office, 1977.
3. Health Security Act, §5120 et seq.
4. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).
5. Jacobson PD. National health information privacy regulations under HIPAA: medical records and HIPAA: is it too late to protect privacy? Minn Law Rev 2002;86:1497-514.
6. Gordon SM. Privacy standards for health information: the misnomer of administrative simplification. Del Law Rev 2002;5:23-55.
7. Zoeller B. Health and Human Services privacy proposal: a failed attempt at health information privacy protection. Brandeis Law J 2002;40:1065-83.
8. Annas GJ. The rights of patients. 2nd ed. Carbondale: Southern Illinois University Press, 1989.
9. Siegler M. Confidentiality in medicine — a decrepit concept. N Engl J Med 1982;307:1518-21.
10. Ladine B. Medical privacy rules are relaxed. Boston Globe. August 10, 2002:A1.
11. Standards for privacy of individually identifiable health information. Washington, D.C.: Office for Civil Rights, Department of Health and Human Services, December 3, 2002:25. (Also available at http://www.hhs.gov/ocr/hipaa/.)
12. Annas GJ. Medical privacy and medical research — judging the new federal regulations. N Engl J Med 2002;346:216-20.
13. Kulynych J, Korn D. The effect of the new federal medical-privacy rule on research. N Engl J Med 2002;346:201-4.
14. *Idem.* The new federal medical-privacy rule. N Engl J Med 2002; 347:1133-4.
15. Federman DD, Hanna KE, Rodriguez LL, eds. Responsible research: a systems approach to protecting research participants. Washington, D.C.: National Academies Press, 2003.
16. Federal policy for protection of human subjects, 45 C.F.R. §46 (June 18, 1991). Fed Regist 1991;56:28003.
17. 42 U.S.C. §1320 D-1.
18. 42 U.S.C. §1320 D-6.