2002

Medical Privacy and Medical Research: Judging the New Federal Regulations

George J. Annas

Legal Issues in Medicine

Medical Privacy and Medical Research — Judging the New Federal Regulations

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

AMERICANS support both protecting the privacy of medical records and encouraging medical research. Thus, it is not surprising that a move to change practices in these two areas has generated attention and comment. The new federal regulations, promulgated under the authority of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), were adopted to protect the privacy of medical records. They were not specifically designed to facilitate or limit medical research.[1] Nonetheless, the regulations have prompted strong objections from the biotechnology industry and from academic medicine. The Association of American Medical Colleges and the Biotechnology Industry Organization have argued that the regulations will make it more difficult, if not impossible, to conduct research involving the use of medical records.[2-4] Kulynych and Korn discuss some of these objections elsewhere in this issue of the *Journal*.[5] In this article, I summarize the new regulations, outline the debate over them, and suggest directions for changes.

The HIPAA regulations and commentary are so detailed and complex that an entire consulting industry has grown up around them — even though compliance is not required until April 2003. In a report on research rules that is more than 200 pages long, the National Bioethics Advisory Commission devoted only one paragraph to the HIPAA regulations. The commission concluded that they provide "little federal guidance for IRBs [institutional review boards] and investigators regarding the protection of privacy and confidentiality" and that they do not apply to all research conducted in the United States.[6] Nonetheless, the basic concept underlying the regulations is clear: so-called covered entities (all health plans, health care "clearinghouses," and health care providers, including all physicians except those who never transmit any health information electronically) must obtain specific, written authorization from a patient to use or disclose health care information (whether written or electronic) that is linked to that patient. Patients must also be notified about their rights with respect to their medical information, including the right to restrict the use and disclosure of such information, the right to inspect and copy their records, the right to amend their records, and the right to an audit of any disclosure of their records. In addition, these entities "must make reasonable efforts to limit health information to the minimum necessary to accomplish the intended purpose" when they use, disclose, or request such information. The new regulations do not preempt or change any existing rule or state law that provides greater protection of privacy.[1]

The new regulations were adopted for three reasons: to give patients access to and control of their medical information, to restore trust in the health care system, and to improve the "efficiency and effectiveness" of health care delivery by adopting a national framework for maintaining the privacy of medical information.[1] None of these goals are controversial. As the background to the regulations notes, previously there were "virtually no federal rules . . . to protect the privacy of health information and guarantee patient access to such information. . . . All fifty states today recognize in tort law a common law or statutory right to privacy."[1] The increasing use of computers and the Internet has also heightened the public's concern that the privacy of medical information is not being adequately protected.[7]

A patient's medical record is seen by an average of 150 people during the course of a hospital stay.[8] No laws specify the people who are allowed to see medical records or the parts of the records they can see.[1] Of even more concern, individually identifiable medical information is frequently shared with managed-care organizations, health insurance companies, life insurance companies, self-insured employers, pharmacies, pharmacy-benefit managers, clinical laboratories, accrediting organizations, and medical-information bureaus.[1] With many multistate organizations involved in health care, there is a need for uniform national standards. The debate is about what those standards should be.[9]

RESEARCH RULES

Since the public strongly supports medical research, it is likely that most people would agree to have their medical records reviewed by researchers if the researchers did not disclose identifiable information to anyone else.[10,11] Obtaining authorization from patients to use their medical records for the purpose of research, however, takes time and effort, and many researchers would prefer not to obtain such authorization from each patient. The new regulations also require authorization in a form that is much more detailed than that previously required. The main argument against requiring individual authorization is that the invasion of privacy by a researcher viewing medical records is minimal, and in effect, no one (other than the researcher) will ever know about it anyway, as long as confidentiality is maintained.

Under current federal regulations (also known as the "common rule"), research protocols and con-

sent forms are reviewed by an IRB.[6,12] The IRB has the authority to waive the requirement of informed consent if it decides that the proposed research involves "no more than minimal risk," that the waiver "will not adversely affect the rights and welfare of subjects," and that "the research could not practicably be carried out without the waiver."[12] These rules for waiving the requirement of informed consent apply to all types of research.

The HIPAA regulations also permit patient authorization to be waived in certain circumstances. A covered entity, such as a hospital, may give researchers access to medical records without IRB review or authorization by individual patients in two specific instances: preparing a research protocol (as long as access to medical records is needed for its preparation and no protected medical information is removed from the site), and performing research that concerns only people who have died.[1] In all other cases, waivers can be obtained only from an IRB or privacy board (a new entity that is substantially similar in composition to an IRB but that has authority only to review "privacy rights and related interests" in the research setting). The following criteria must be satisfied to grant a waiver:

(A) The use or disclosure of protected health information involves no more than minimal risk to the individuals;
(B) The . . . waiver will not adversely affect the privacy rights and welfare of the individuals;
(C) The research could not practicably be conducted without the . . . waiver;
(D) The research could not practicably be conducted without access to and use of the protected health information;
(E) The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;
(F) There is an adequate plan to protect the identifiers from improper use and disclosure;
(G) There is an adequate plan to destroy the identifiers at the earliest opportunity. . . ;
(H) There are adequate assurances that protected health information will not be reused. . . .[1]

Of course, if information cannot be linked to an individual patient, disclosure or use of the information cannot violate the patient's privacy. The regulations provide two methods for the "de-identification" of medical information. The first is for a knowledgeable statistician to determine that the risk of identifying an individual patient from the information disclosed or used is "very small" and to document the methods and results used to arrive at this conclusion. The second method is to strip the records of the following identifiers: name, address (although the first three digits of the ZIP Code may be retained if the geographic unit contains more than 20,000 people); telephone and fax numbers; e-mail address; Social Security, medical-record, health plan, and account numbers; certificate, license, vehicle, and medical-device serial numbers; World Wide Web universal-resource-locater (URL) and Internet-protocol (IP) numbers; biometric identifiers (including fingerprints and voiceprints); full-face photographs; and "any other unique identifying number, characteristic or code."[1]

OBJECTIONS TO THE NEW RULES

Arguing that "the public interest in the discoveries and findings of research is as strong as the public interest in medical privacy," the Biotechnology Industry Organization has stated that privacy rules should be crafted "so as not to adversely affect research."[3] In a letter to the Department of Health and Human Services, the organization said that its members were "shocked and deeply disappointed that the proposed regulation failed at every turn to establish a legal framework that would serve both objectives."[3] The organization argued, among other things, that the de-identification provisions are "unrealistic" and should be modified and supplemented by a rule that permits covered entities "to use valid statistical methods for creating databases that may be treated as de-identified."[3] Moreover, deleting the 18 specific identifiers, the organization argued, "would result in medical history data of questionable completeness, raising serious doubts about the validity of conclusions drawn from any research using a de-identified database."[3]

The response of the Association of American Medical Colleges to the new regulations has focused on making them more hospitable for researchers. The association recommended that the list of identifiers that must be removed from medical records be reduced from 18 to 8 (name, address, telephone number, fax number, e-mail address, Social Security number, vehicle number, and full-face or profile photograph), as long as the covered entity did not have "actual knowledge" that the disclosed information could be used alone or in combination with other available information to identify an individual patient.[2] With respect to the other means of ensuring privacy — the determination that the risk of identification of an individual patient would be "very small" — the association proposed that the covered entity make this judgment, not a statistician. Finally, the association asked that an exception to the requirements be made for health information disclosed to a researcher who provides written assurance that "the information will be used only for research purposes and will not be further disclosed except as required by law" and that there will be no "attempt to re-identify or contact individuals who are the subjects of the information."[2]

The Association of American Medical Colleges also objected to the criteria for an IRB's waiver of the authorization requirement, arguing that criteria B and E are contradictory and that these requirements could not be reconciled by an IRB.[2,13] Moreover, there is a major difference between the requirements for a waiver under the common rule (which applies to all research protocols, not just those involving access to medical records)[12] and the HIPAA regulations. As Barnes and Krauss have pointed out, the common rule addresses the "overall welfare and interests" of research subjects, whereas the HIPAA regulations "pertain only to research subjects' privacy interests."[14]

New Authorization Requirements for the Release of Medical Information

Researchers might prefer that their access to medical records be unimpeded so long as they agree not to disclose identifiable information to others. Easy access to medical records might also benefit public health and law-enforcement officials. Thus, the HIPAA regulations, promulgated at the end of the Clinton administration, came as a surprise, at least as they apply to medical research.[15] Even more surprising was the endorsement of the regulations by the Bush administration.[16] With such bipartisan support, it is likely that a version of the regulations that is very close to the current version will take effect in 2003.

The new regulations require that research subjects sign a form authorizing the use and disclosure of their private medical information. Theoretically, at least, subjects have always had to be asked to consent to the use of their medical information in research. But such consent is often vague, as are existing IRB rules for protecting privacy, which require only that "where appropriate there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data."[6,12] Under the HIPAA regulations, the required authorization is much more specific. It must be in writing and must contain at least the following elements:

(i) A description of the information to be used . . . in a specific and meaningful fashion;
(ii) The name or other specific identification of the person(s) . . . authorized to make the requested use or disclosure;
(iii) The name . . . to whom the covered entity may make the requested use or disclosure;
(iv) An expiration date or an expiration event. . . ;
(v) A statement of the individual's right to revoke the authorization. . . ;
(vi) A statement that the information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by [the HIPAA];
(vii) Signature of the individual and date.[1]

Specification of an expiration date or event ("conclusion of the research project" might suffice) and the right to revoke the authorization are the most unusual provisions. Of course, all subjects have the right to revoke their agreement to participate in research at any time.[12] However, the ability of the subject to set an expiration date or event for the authorization is new. Also new is the provision under HIPAA that all persons have a right to obtain access to their medical information (a right that may not explicitly be provided under existing laws and that, even if it is, may not apply to research records).[1] Thus, subjects could obtain access to research information (such as whether they were in a placebo group) after revoking authorization, unless other provisions were explicitly made in the authorization.

None of the HIPAA provisions for authorization necessarily impede research, and they can usually be integrated into the informed-consent form that subjects must sign before participating in research.[1] It should be emphasized, however, that "informed consent is not a form" but a process.[6] As I have written in the context of genetic research, sole reliance on complex consent forms to protect research subjects will only add to the bureaucracy and red tape surrounding research without increasing the subjects' understanding or safeguarding their rights.[17]

A Broader View

The critics argue that under the HIPAA regulations, IRBs will be less able (or willing) to waive the requirement for individual consent to perform research involving medical records than they currently are under the common rule. In my view, this argument ignores the broader issue of whether such research should be permitted without the requirement of individual consent. The question is not whether it takes more time and effort to obtain individual authorization but whether the individual privacy rights that are being protected by requiring such authorization are important enough to warrant the requirement. Only the public can answer this question. If it turns out that there are virtually no refusals to authorize the use of identifiable medical records in research and that there are no "leaks" of medical information in research trials, the requirement could be reconsidered. The HIPAA regulations are based on the premise that the public does care. This premise is supported by survey data, cited in the background to the HIPAA regulations, showing a high level of public concern about the privacy of medical records.[1] Of course, even if no one refuses to participate in a research project involving medical records, people may still want to be asked for their approval in advance.

Because many researchers do not want to obtain individual authorization to use or disclose private

medical information, the mechanisms for obtaining an exception to this requirement — seeking a waiver from the IRB or privacy board and eliminating identifiers from medical information — are important. Both the Biotechnology Industry Organization and the Association of American Medical Colleges believe that the rules for eliminating identifiers are too strict and that the remaining medical information would be much less useful than information with more identifiers.[3,6] This concern is understandable — researchers often want to collect as much information as they can, since they may not know which data will ultimately be important.

The HIPAA regulations permit researchers to retain all the identifiers with the patient's authorization. It is only in the absence of such authorization that 18 specific identifiers must be stripped to provide legal protection against the charge of a violation of privacy. To argue that some of these identifiers can be retained without the patient's authorization is essentially to argue that it is not necessary to remove such information in order to protect privacy. The regulations, however, are based on the opposite premise. The alternative approach is for an expert to assess the overall risk of patient identification. The requirement that an expert in statistics make this assessment has been criticized, but who else other than such an expert could realistically and reasonably make it?

In my view, the new provisions for a waiver of the authorization requirement should be used sparingly, since the goal of the regulations is to bolster public trust by protecting privacy, not to make it easier to perform research involving the use of medical records. Nonetheless, the Association of American Medical Colleges and others have raised reasonable questions in this regard. Specifically, how can criteria B and E be reconciled — that is, how can the proposed research "not adversely affect the privacy rights and welfare of the individuals" and at the same time entail "risks to individuals . . . [that are] reasonable in relation to the anticipated benefits"? If the research poses no risks, then criterion E is unnecessary, but if the research does pose risks, then criterion B cannot be met. Clarification is required, although deleting either criterion B or criterion E seems more reasonable than deleting both, as the Association of American Medical Colleges has suggested.

Criterion G specifies that when the identifying information is no longer required for the research, it will be destroyed. This requirement is perfectly reasonable. It also seems reasonable for the IRB (or privacy board) to establish a specific date or event that will trigger the requirement, since the subjects will not be personally involved in the research and are therefore unlikely to know when it is finished.

CONCLUSIONS

Although the National Bioethics Advisory Commission did not analyze the new HIPAA regulations as they relate to research, it made some important relevant points. First, the commission stated that "federal policy should be developed and mechanisms should be provided to enable investigators and institutions to reduce threats to privacy and breaches of confidentiality. The feasibility of additional mechanisms should be examined to strengthen confidentiality protections in research studies."[6] Second, noting that much of the research performed in the United States today is not subject to the common rule, the commission recommended that Congress require all research to be subject to the same rules.[6] Finally, the commission called for reform of the IRB system, including the establishment of an independent agency to oversee IRBs and greater representation of the public on the boards.[6]

I believe this reform process must include revisions of the common rule, including its vague, one-sentence provision regarding privacy. In rewriting the common rule, it will be important to take into account the new HIPAA regulations and the reactions of the research community. Ultimately, it is the federal research rules, not the HIPAA regulations, that should provide guidance for IRBs. In the meantime, efforts should be focused on developing constructive ways to implement the HIPAA regulations (including amending them where appropriate) rather than trying to return to the days when privacy was not taken seriously in medical research. Public support of medical research really is a function of public trust. Providing meaningful protection of the privacy of medical records in research is an important goal in its own right and will also increase public trust in the entire medical-research enterprise.

REFERENCES

1. Department of Health and Human Services. Standards for privacy of individually identifiable health information. Final rule. Fed Regist 2000; 65(250):82462-829.

2. AAMC comment letter on DHHS final rule on "Standards for the Privacy of Individually Identifiable Health Information." Washington, D.C.: Association of American Medical Colleges, March 30, 2001. (Accessed December 27, 2001, at http://www.aamc.org/advocacy/testimny/research/hipaathompson.htm.)

3. Comments on proposed standards for privacy of individually identifiable health information. Washington, D.C.: Biotechnology Industry Organization, February 15, 2000. (Accessed December 27, 2001, at http://www.bio.org/laws/comments021700.html.)

4. Kaiser J. Researchers say rules are too restrictive. Science 2001;294: 2070-1.

5. Kulynych J, Korn D. The effect of the new federal medical-privacy rule on research. N Engl J Med 2002;346:201-4.

6. Ethical and policy issues in research involving human participants. Bethesda, Md.: National Bioethics Advisory Commission, August 2001.

7. National Research Council. For the record: protecting electronic health information. Washington, D.C.: National Academy of Sciences, 1997.

8. Siegler M. Confidentiality in medicine — a decrepit concept. N Engl J Med 1982;307:1518-21.

9. Welch CA. Sacred secrets — the privacy of medical records. N Engl J Med 2001;345:371-2.
10. Melton LJ III. The threat to medical-records research. N Engl J Med 1997;337:1466-70.
11. Yawn B, Jacobsen SJ, Geier GR Jr. Who proves and who denies authorization for medical record review for medical research. Presented at the National Center for Health Statistics Conference/Joint Meeting of the Public Health Conference on Records and Statistics and Data Users Conference, Washington, D.C., July 29, 1997.
12. Protection of Human Subjects, 45 CFR 46 (June 18, 1991).
13. Researchers: privacy rule creates obstacles, needs fixing. Montgomery Village, Md.: Phoenix Health Systems, August 21, 2001. (Accessed December 27, 2001, at http://www.hipaadvisory.com/news/2001/aamc0827.htm.)
14. Barnes M, Krauss S. The effect of HIPAA on human subjects research. BNA's Health Law Reporter. June 28, 2001:1026-41.
15. Pear R. Rules on medical privacy. New York Times. December 24, 2000:D2.
16. Southwick R. Colleges fear impact of U.S. privacy rules on medical research. Chronicle of Higher Education. April 27, 2001:31.
17. Annas GJ. Reforming informed consent to genetic research. JAMA 2001;286:2326-8.