Proposed Federal Legislation Jeopardizes Patient Privacy

Steven K. Hoge, MD

In the last year there has been a move to enact federal legislation concerning private health-care information. This move has been fueled by a growing trend toward the computerization and electronic transmission of health-care information. These advances in technology call for appropriate new protections of patients' privacy. Unfortunately, the proposed legislation has not received adequate attention in the medical community. Physicians and patients in general are not aware of the legislation and have not been engaged in shaping its contents. In its current form, the legislation would seriously undermine traditional protections of confidentiality that are ensured by physicians. The flaws of the proposed legislation are examined in this article.

The public's concern about the protection of medical records is high, and understandably so: health care information includes personal details of the most private nature. Historically, physicians have recognized the importance of patient privacy; the duty to maintain confidentiality has been a constant in medical ethics and a cornerstone of the doctor-patient relationship.[1,2] Therefore, it would be expected that proposed federal legislation that would seriously affect patient privacy would generate considerable discussion in the medical community. Yet, last year the 103rd Congress attracted little attention when it considered comprehensive amendments to President Clinton's proposed Health Security Act (House of Representatives (H.R.) 3600) that would have created a national system of data banks to house medical records and would have replaced existing state laws governing confidentiality with a single, national statute.[3]

Although these amendments ultimately died in the 103rd Congress along with health care reform, similar legislation has been introduced in both houses of Congress in the current session under Title IV of the Family Health Insurance Protection Act (Senate (S.) 7), the Fair Health Information Practices Act (H.R. 435), and Title II of the Basic Health Care Reform Act (H.R. 1234).[4–6] These bills appear to be politically viable.[7,8] It is imperative that physicians begin to consider the merits of the proposals. Discussion of data banks within the medical community is urgently needed; even in the absence of

Dr. Hoge is affiliated with the Schools of Medicine and Law, University of Virginia, Charlottesville, VA. Address correspondence to: Steven K. Hoge, MD, University of Virginia, School of Law, 580 Massie Rd., Charlottesville, VA 22903.

legislation, private data banks are expanding, and regulatory agencies have begun to consider electronic forms of storage and transmission of health-care information as part of a national information infrastructure.[9] The legislation that addresses health-care confidentiality—S. 7 and H.R. 435—has evolved over the course of two Congressional sessions, and its provisions reflect a series of compromises between ready access to medical information and patient privacy. Each of these policy judgments deserves careful scrutiny. As written, the bills contain provisions that would seriously undermine traditional medical ethical duties and would strip patients of important privacy protections.

Medical Data Banks

The 1994 proposed legislation would have granted the Department of Health and Human Services (HHS) broad authority to specify "data elements" from patients' records to be reported and stored in a health information network of regional data banks. Containing comprehensive patient information, the data bank system would have been the nerve center of the reformed health-care system and would have facilitated the transfer of records, outcomes research, and detection of fraud and abuse. As originally conceived, the data banks would have stored medical dossiers consolidating all electronically filed details of health-care information from birth to death, across health-care providers for everyone in the United States.[3, 10]

While the goals of the legislation currently under consideration appear to be more modest—the facilitation of electronic communication—in actuality S. 7 would establish the legislative framework for the creation of a data bank system. To facilitate the flow of patients' health care information, public or private entities would translate medical records into electronic data elements (in the Senate version of the bill, these entities are termed Health Information Protection Organizations (HIPOs) and in the House of Representatives version, Health Information Security Organizations (HISOs)).[5, 6] Each patient, provider, and health plan would be assigned a "unique identifier." The HIPOs would store the electronic health information specified by HHS and facilitate its transmission to health-care providers, government agencies, and other HIPOs. The Health Information Network would arise from this web of communication.

HHS would be authorized to establish standards for electronic transmission of health care data. Once these standards have been developed, all health-care providers would be required to conduct their transactions with health plans and agencies in the standardized electronic format. In addition to claim-related data, HHS would be given authority to establish standards for the transmission of data "consistent with the goals of improving the health care system and reducing administrative costs."[11] This delegation of authority is written so broadly that it could encompass all information in patients' files.

Once HHS establishes standards for electronic transmission, any federal or state agency request for that information

must be honored. In essence, the bill would authorize governmental agencies to requisition information from the Health Information Network. Because the information to be provided to government agencies would have identifiers removed, the threat to patients' privacy would be reduced.

The availability of an electronically transmissible medical record for every individual would have obvious advantages. Driving the creation of the Health Information Network is the prospect that governmental oversight agencies will be able to detect patterns of medical fraud from reported data. Most importantly, physicians would have quick access to medical records.[10]

Unfortunately, in moving to a system of computerized access, many privacy protections inherent in traditional medical record keeping would be lost. The traditional medical record room poses substantial obstacles to illicit perusal. Those seeking to inspect records must have authorization and must view records in person. Moreover, because paper records are not centralized (a single patient's records may be fragmented across a number of health-care providers), in the event of a breach in security, illicit access will be limited. Indeed, patients who are especially concerned about privacy may seek services away from home or from their regular physicians in order to compartmentalize medical information. Electronic storage of medical information opens the potential for access to the universe of people with the ability to gain entry to the data bank. Through remote access, patients' records may be viewed anonymously, and once access is gained, comprehensive information will be available. The threat to privacy is increased by computer technologies that free users from case-by-case browsing. In the time necessary to read a single medical record, thousands of computer files can be scanned or simply copied for later inspection.[12] While traditional medical record storage systems are fallible, it is clear that the electronic storage of medical information poses threats to privacy of a different order of magnitude.

Security protections for computerized data have been notoriously ineffective. An active black-market trade in computerized information exists.[3, 13, 14] Medical information and government databases have not been immune to illicit access.[3, 13, 15] Some patients are aware of the threat to their privacy posed by current, limited medical data banks and opt not to use their medical insurance to avoid privacy intrusions. This option will not exist under the proposed legislation.

Federal Confidentiality Provisions

The proposed federal legislation, captioned the Fair Health Information Practices Act (FHIPA) in the House of Representatives version, would create a national standard for the protection of medical information. FHIPA is comprehensive in scope, covering patient-authorized access to information, patient access to records to correct errors, disclosures among health-care providers, and the communication of information to researchers, oversight agencies, public health officials, and the public.[3] Some

commentators have argued that a uniform national standard would streamline the functioning of health-care systems, which increasingly operate across state lines.[10] In many respects, the provisions of FHIPA provide substantial safeguards to patient confidentiality. Unfortunately, FHIPA would create a disclosure scheme that would discard the protections of patient confidentiality provided by physicians. In addition, FHIPA would grant law enforcement agencies access to medical information.

Traditionally, physicians have controlled access to medical records. As the guardian of confidential medical information, physicians have protected patients' privacy from unwarranted intrusions that might result from unauthorized or authorized disclosures.[16–18] When disclosures are sought by others, physicians refuse inappropriate access. In cases in which right to access is uncertain, physicians have acted as sentinels, alerting patients that others are seeking to obtain their records. Physicians may take steps to protect records, even in the face of legal pressures. Moreover, physicians, aware of the misuses of medical information by third parties, have offered guidance to patients so that voluntary disclosures of medical information are tailored to meet the needs of third parties and minimize privacy intrusions. The American Medical Association has reaffirmed the importance of physician control of medical information in guidelines governing the confidentiality of computerized data.[19]

The role of physicians in safeguarding patients' privacy includes protecting the records from the scrutiny of law enforcement agencies. Courts have recognized the authority of physicians to object to law enforcement seizures of records; patients cannot object to these seizures unless they forgo the privacy they seek to protect.[16–18] Currently, procedural safeguards ensure that law enforcement agencies are seeking medical information for legitimate purposes and that the rights of patients are balanced against investigatory needs. Law enforcement agencies must seek judicial authorization to obtain access to records and, except in extreme circumstances, before a court order is granted, patients and their doctors must be notified that records are being sought so that they have the opportunity to oppose the release of information. Law enforcement agencies bear the burden of proving in an adversarial hearing that the records contain information relevant to a legal inquiry. Some states provide more stringent protections; for example, requiring proof that the requested information is not available through another source. In many cases, judges will deny access or, when law enforcement access is granted, will limit agencies' access to information to ensure that patients suffer the least possible intrusion into their privacy.

The drafters of FHIPA, ignoring the traditional role of physicians, have eliminated the requirement for physician authorization of significant disclosures. Under FHIPA, physicians may not be aware that medical records have been disclosed, even after the fact.[4,5] To enhance the ready flow of health-care information, the bill authorizes the release of information by HIPOs/HISOs and by health-care plans, insurance companies, or oversight

agencies that obtain medical information from physicians on the Health Information Network. Moreover, FHIPA authorizes law enforcement agencies' access to private medical information without judicial oversight and without requiring notification to physicians or patients. Under this latter provision, the police could gain access to hospital and clinic files when they are looking for evidence of crime or trying to locate fugitives. For example, the police might require access to all obstetric/gynecologic records of females under the age of consent when in search of evidence of statutory rape; or in pursuit of fugitives, the police could scan all medical records on a daily basis.

These key provisions of FHIPA represent significant departures from existing norms of medical practice and legal due process. The broad grant of authority to law enforcement agencies to seize medical information and, through databases held by health oversight agencies and health plans, to cast a wide surveillance net is constitutionally suspect.[18] Whatever the legality of these provisions, they substantially diminish patients' privacy.

Conclusion

Medical societies have watched the advances in the use of information technologies with growing concern for patient privacy. As new technologies have come on-line, existing laws, regulations, and practices have become increasingly outdated.[10, 20] In the private sector, significant difficulties in protecting the privacy of patients' computerized health-care data have emerged.[21, 22] It appears that federal regulation will be necessary to safeguard the information contained in existing computer data banks.[10] However, the creation of a national Health Information Network authorized to store medical information represents a major step in the storage and centralization of health-care data. The public discussion and debate that should attend such a development have not yet taken place. This is a major crossroads for the issue of patient privacy in the United States, and the public needs to be educated and engaged by the medical community in discussion. Presently, the public is largely unaware of the proposed legislation. The bill has received no national media exposure and a recent article on patient privacy in a major consumer publication failed to discuss the legislation while it was under consideration in Congress.[23]

Several questions need to be raised and addressed in these discussions. Do we need a national data bank? If data banks are desired, what information should they store? What limits should be placed on governmental access to health-care data? What security measures are necessary to protect this information and how effective are they? Should everyone be required to participate? Why should individual patients not have the opportunity to designate information as off-limits to computerized databases? The public needs to address these questions in order to make an informed decision that reflects reasonable trade-offs between privacy and other interests.

A similar public discussion should focus on the merits of FHIPA. It has been suggested that a federal confidentiality statute would remedy the gaps in the pro-

tection of medical records that exist in some states' laws.[10] However, this may not be true, since the legal analysis that served as a basis for this conclusion did not take into account case law and common law protections, nor did it consider the prevailing standards of care in medical practice or ethical norms that safeguard confidentiality. It is clear, however, that FHIPA is seriously flawed and would result, in some areas, in less stringent protections of patients' confidentiality than is now provided in many states.

Physicians should be prepared to discuss the issue of confidentiality with their patients and should take an active role in the debate to ensure that traditional medical values are preserved.

References

1. Ludwig E: The Hippocratic Oath: Text, Translation and Interpretation. Baltimore: Johns Hopkins Press, 1943
2. American Medical Association: Principles of Medical Ethics. Chicago: AMA, 1992
3. Health Security Act, H.R. 601, Part 5, 103d Cong, 2d Sess, August 12, 1994; S. 1779, Subtitle B, Information Systems and Privacy, 103rd Cong, 2d Sess, 1994
4. H.R. 435, introduced January 9, 1995
5. S. 7, introduced January 4, 1995
6. H.R. 1234, introduced March 14, 1995
7. Bureau of National Affairs Health Care Policy Report: Republican leaders likely to pursue scaled-back reforms in new Congress. November 21, 1994, pp 1919–20
8. Bureau of National Affairs Health Care Policy Report: Rep Thomas sees modest series of health reforms in 104th Congress. January 2, 1995, p 6
9. HCFA Public Hearing: Security for education and health information in the National Information Infrastructure. Washington, DC, December 8, 1994
10. Gostin LO, Turek-Brezina J, Powers M, Kozloff R, Faden R, Steinauer DD: Privacy and security of personal information in a new health care system. JAMA 270:2487–93, 1993
11. S. 7, Sec 4012 (a)(2)
12. US Congress, Office of Technology Assessment: Protecting Privacy in Computerized Medical Information (OTA-TCT-576). Washington, DC: US Government Printing Office, 1993
13. Privacy: Your Secrets for Sale (pts 1 and 2). ABC News Nightline. June 9–10, 1994
14. Rothfeder J: Privacy for Sale: How Computerization Has Made Everyone's Life an Open Secret. New York: Simon and Schuster, 1992
15. Medical Data Gathered by Firms Can Prove Less than Confidential. Wall Street Journal. May 18, 1995, p A1–5
16. In re "B," 394 A.2d 419 (Pa 1978)
17. Commonwealth v. Kobrin, 479 N.E.2d 674 (Mass 1985)
18. Hawaii Psychiatric Society v. Ariyoshi, 481 F Supp 1028 (D Haw 1979)
19. Current Opinions of the Council on Ethical and Judicial Affairs of the American Medical Association: Confidentiality: computers. Report 5.07, 1992
20. Institute of Medicine: Health Data in the Information Age: Use, Disclosure, and Privacy. Washington, DC: National Academy Press, 1994
21. Bass A: HMO puts confidential records online. Boston Globe. March 7, 1995, p 1
22. Bass A: HCHP reviewing policy on records: privacy at issue on doctors' notes. Boston Globe. March 9, 1995, p 1
23. Who's Reading Your Medical Records? Consumer Reports. October 1994, pp 628–32