The Cost of HIPAA Compliance

Peter Kilbridge, M.D.

The deadline for compliance with the regulations for patient privacy in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is now upon us, and hospitals and physician groups are in the throes of working to meet it. This is an enormous chore, affecting numerous areas of hospital operations and, ultimately, every employee.

Meeting the requirements of the extensive privacy regulations — the deadline for which is April 14, 2003 — has been consuming substantial time, resources, and energy from hospitals and physician groups. For example, essentially all employees must be trained in the protection of patients’ privacy, and their completion of this training must be documented. The training focuses on practices for handling protected health information: for example, avoiding discussing patients within the hearing of others, locating fax machines and printers in secure areas, and obtaining only the information about a patient that is required for the job at hand. Some hospitals have developed their own materials in the form of scenario-based videos or computer-based productions. Others have brought in outside educators or opted to conduct face-to-face classroom training.

A study commissioned by the American Hospital Association in 2000 estimated the average cost of training at $16 per employee.

HIPAA requires that a notice of privacy be given to every patient, informing him or her of, among other things, the organization’s usual uses of information about patients and patients’ rights with regard to their records. The privacy notice, among other aspects of the requirements, is discussed by Annas in this issue of the Journal (pages 1486–1490). The notice must be presented to every patient at his or her first appearance for care after the April 14 deadline, and the patient’s acknowledgment of receipt of the notice must be recorded. Even for a small hospital, just the cost of printing a multipage form for every active patient, at a few cents apiece, is substantial. Organizations with multiple locations for care delivery must deal with the added costs of duplication of materials and effort, since some patients will receive more than one notice if they visit multiple locations. In addition, such organizations face the challenge of keeping a consolidated record of which patients have received the notice. Many organizations are investing in new information systems to manage this massive tracking effort.

Physicians’ offices and clinics must effect behavioral change in the practice setting. Physicians and nurses may not talk with patients about diagnostic and care information in public areas. Members of the office staff must conduct telephone and other conversations in a manner that reduces their use of information that identifies particular patients. If chart racks are located in hallways outside clinic rooms, the charts should be placed with the patient information facing the wall. Physicians must attend to the details of office layout and logistics as well. It may be necessary to move waiting-room seats some distance from the administrative area to reduce the likelihood that patients will overhear conversations; it may be necessary to play music or run white-noise machines in order to obscure the sound of conversations in clinic rooms. Computers may need to be relocated away from hallways or to be equipped with screens that inhibit casual viewing by passersby.

Organizations are required under the privacy regulations to track all disclosures of patient information for uses beyond treatment, payment, and operations. In order to do so, they must first determine what constitutes a disclosure for a use beyond normal operations (for example, is a particular request for a record being made for the purposes of quality improvement — which is considered a normal operation — or for research purposes?). They must establish policies and procedures for making these determinations. And they must construct a system for tracking every such release — whether of paper records or electronic information. Tracking the release of electronic information will most likely require the purchase of a computer program designed for this purpose and the implementation of the system in a fashion that ensures the capture of all instances of disclosure, from any site where care is provided.

Other challenges in the implementation of com-
Compliance with the HIPAA regulations include the potential need to revise contracts with all “business associates” to bind these parties to HIPAA privacy practices; the management of hospital directories (patients have the right to determine whether and how they wish to be listed in the patient directory when they are admitted to the hospital); the management of amendments to patient records; the implications of the regulations for clinical research; implications for hospital fundraising (physicians have to obtain authorization from patients for the release of information to development officers); and resolution of issues regarding preemption by state law. In addition, considerable resources are being devoted to the implementation of standards for electronic transactions and to the implementation of newly released electronic security requirements.

The magnitude of the overall challenge is reflected in the winter 2003 survey of HIPAA readiness conducted by the Healthcare Information and Management Systems Society and Phoenix Health Systems. As of January 2003, only 9 percent of 467 provider organizations responding to the survey indicated that they believed they had achieved compliance with the privacy rules. The survey also showed that there was broad agreement that the most difficult aspect of the process was understanding and interpreting the regulations and that hospitals tend to use outside consultants primarily for assessment and planning activities, tackling the greatest portion of the work — implementation — with internal resources. Estimated spending to comply with HIPAA varies greatly among organizations (see Figure).

The results of the survey are in line with those cited by the organizations that I interviewed, and many organizations agreed that the financial outlay required — although it is substantial — has been somewhat smaller than they anticipated. The 2000 American Hospital Association study cited above estimated that the average cost of compliance per hospital ranged from about $670,000 to $3.7 million — considerably more than the figures in the 2003 survey suggest. Modifications of the regulations in the past year clearly contributed to the difference, but perhaps the most important reason for the discrepancy is that although most hospitals and large practices have had to hire or commit one or several full-time employees (such as a privacy officer) to heading up the compliance effort, the majority of the work is being done with existing resources — while other initiatives are put on hold.

What is being accomplished with all this effort? The extensive privacy regulations enforce the adoption of privacy-conscious behavior by caregivers and employees of hospitals and health care practices — an area in which medicine has historically been rather lax; and greater attention should be paid to safeguarding privacy in an era of universal electronic communication and increasing computerization of confidential patient information. On the other hand, some of the regulations seem excessively burdensome — such as requiring the tracking of every disclosure of information for uses beyond treatment, payment, and operations and recording the acknowledgment of receipt of an 8-to-20-page informational document that most patients will throw away without reading. One thing is certain: many organizations will breathe a sigh of relief when HIPAA compliance is behind them.