The HIPAA-potamus in Health Care Data Security

Regulations intended to improve health care data access have created new security risks along with headaches for patients and practitioners.

Deadlines for compliance with the Health Insurance Portability and Accountability Act (HIPAA) have caused a major crunch for the computer security industry. This hippopotamus-sized legislation, enacted in 1996 (see cms.hhs.gov/hipaa) consists of two major provisions: insurance reform (so that preexisting conditions do not result in denial of coverage when one changes jobs); and administrative simplification (intended to reduce health care costs through standardized electronic transmission of transactions). HIPAA violations can carry fines of up to $250,000 and jail time of up to 10 years, so you can bet that organizations are taking this federal law very seriously.

Like many legislative initiatives, HIPAA appears to have been intended to reduce costs (in this case, insurance-related health transactions for patients) but the overhead of compliance generally has the opposite effect. Here, since it was anticipated that information violations could be more likely to occur through electronic data collection and consolidation, privacy was specifically mandated in the regulations. And therein lies the rub, since privacy is an information-age luxury (certainly not free). HIPAA's Privacy Rule component addresses the use and disclosure of Protected Health Information (PHI) by health care plans, medical providers, and clearinghouses. The U.S. Department of Health and Human Services explains that "a major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's health and well being" [4].

This privacy rule finds its manifestation in the ubiquitous "Notice of Privacy Practices Patient Acknowledgement" form that one is typically required to sign before receiving medical attention from most U.S. health care service providers. This form purports to attest that the patient (or guardian if a minor) has received information (typically via an accompanying explanatory brochure) regarding the use and disclosure of one's health care information. But the reason for this form, and the use of the personal data to which it relates, has a much broader impact. Typically, health information is provided to others, beyond the medical practitioner's office, for treatment or pay-

JASON SCHNEIDER

Thankfully, existing computer security guidelines and programs are being used to assist with the HIPAA security deployment process.

ment purposes. But few realize it may also be released, without the patient's consent or authorization, to law enforcement, court agencies, the military, public health organizations, and the Food and Drug Administration, among others. Estimates indicate that as many as 150 to 400 individuals may have access to the data collected in a person's medical records [2].

What the patient isn't told (but which I recently discovered while dealing with a major health crisis involving a close relative) is that consent to the privacy form can mean that close family members may not be able to get copies of the contents or summaries of the medical records, even if such access to the information is necessary in order to obtain treatment or payments. Information about other patients treated by the same practitioner can also now be difficult to access, even when malpractice concerns should require some anonymous disclosures.

Gilian Technologies (see www.gilian.com), a HIPAA compliance provider, notes that "full compliance requires these entities to understand the threats and liabilities to this protected data and to ensure they implement a wide variety of safeguards and security best practices." Although HIPAA pertains to all forms of PHI (verbal, paper, and electronic), currently only the electronic formats are addressed in the Security Standards Final Rule published in February 2003.

Businesses have been scurrying to implement compliance programs since the issuance of the Security Rule, since the deadline was originally April 21, 2004. As this date loomed, it became apparent that smaller or less-funded health service organizations (such as local clinics) were considerably behind the learning curve in their ability to comply. Congress granted a one-year extension to smaller plans (until April 2005) and a further 12-month extension may be provided. Compliance is neither simple nor straightforward. For example, information relayed by fax or photocopied may be at risk of exposure through the device storage and print mechanisms. Someone buying a used copier or handling recycled fax cartridges may uncover a PHI bonanza. Such aspects of document security are being addressed by most of the major replication equipment suppliers, including Canon, Konica, Ricoh, and Sharp, through solutions ranging from encryption and firewalls to actual mechanical shredding of hard drives and other components.

Thankfully, existing computer security guidelines and programs are being used to assist with the HIPAA security deployment process. The ISO Common Criteria (CC), originally an outgrowth of the National Institute of Standards and Technologies TCSEC/ITSEC standards required primarily for the security aspects of national defense-related projects, has found considerable applicability within the health care setting, first for equipment design and construction and, more recently, for records-keeping, such as that related to HIPAA-covered data transfers (see www.commoncriteria.org).

All four of the document replication companies mentioned previously have pursued CC certification, and many other health industry products are seen as cutting-edge in obtaining CC ratings. For example, Persona 5.0, a terminal emulation and host access product produced by the French corporation Esker (see www.esker.com), was the first such program to receive CC Evaluation Assurance Level 3 certification. Many companies find overlaps between industries when

they obtain CC status, and Persona is compliant with certain U.S. Department of Defense policies, as well as the Internet security policy requirements of the U.S. Health Care Financing Administration. Alacris, Inc. also received CC certification for its Identity Validation Client, used for security certificate status request management and integrity assurance in pharmaceutical and health care applications, as well as in financial services and government venues (see www.alacris.com).

But solutions are not as simple as adding on security tools and "providing employees with policies and procedures for their job classification and requiring them to read and sign off on them." Former DARPA CIO David Thompson warns purchasing agents to "Beware of snake oil salesmen. Anyone who says that their 'product will make you HIPAA-compliant' is selling false hope. Compliance is not sold in a bottle" [3]. During the initial assessment period, for example, an office may discover that the organization they have contracted with for records retention has subcontracted work to an offshore unit that may leave information vulnerable to disclosure.

A phased-in approach is recommended, even though time is tight, so that any such subsequently revealed noncompliance issues can be appropriately addressed. Implementation must be understood within the health care context, where an extremely stratified set of job roles, and allowances for high-ranked individuals accustomed to doing things in particular ways, has set the tone for the prevailing work environment. Since developing strategies for HIPAA compliance are necessarily time-consuming, it is suggested that the phased approach will also assist in allowing the workers a sufficient period in which to incorporate the new structures and rules into their culture and ethics. Otherwise efforts may be frustrated and unsuccessful.

HIPAA requires the full involvement of every member of the health service group, not just those who are responsible for data processing tasks. Effective HIPAA administration necessitates that each organization develop a management infrastructure with well-defined roles that will address administrative, physical, and technical safeguards. Included must be assessment and mitigation of security and privacy risks, policy and procedures development, incident response and recovery, evaluation of business associate contracts, hiring and termination impacts, compliance and awareness training, access control and authentication, auditing, periodic review, and so on.

Although HIPAA rules tend to be viewed in terms of confidentiality (where privacy violations are related to inappropriate use or disclosure), integrity and availability are also covered under HIPAA. Denial-of-service attacks (via Internet worms or viruses), equipment malfunctions (for example, involving file deletion or corruption of data), and a lack of contingency plans (pertaining to offsite backup, data restoration procedures, and similar activities) may also trigger HIPAA violations. Advances in computer technology have expanded the contents of medical data well beyond simple treatment and drug records—PHI files now may also include the electronic versions of such things as CAT scans, X-rays, EKG tapes, blood and DNA analyses, psychological profiles, and so on—pretty much an entire work-up of your being, once sufficient diagnostic data has been collected.

Even a person's whereabouts during medical procedures can be tracked—for example, at one point during the hospital stay, my relative was positioned in a corridor while waiting for admission, and the computer had his location as "Room 225-Hall" so that nurses knew where to find him. On another occasion, a staff person stopped by with a handheld device to register meal choices. One's doctor is now only a key-click away from patient files, as newly deployed physician portals allow remote file review via the Internet. HIPAA is broadly applied to encompass all of this data and related channels of information exchange, because confidentiality, integrity, and availability (or lack thereof) may

have life-or-death consequences.

User identity management poses an especially large problem, as one might imagine. Scott Ogawa, chief technology officer at Boston's Children's Hospital, reported at the 2003 Inside ID conference that, prior to HIPAA, notes with access codes stuck on monitors in the intensive care unit were commonplace, and that resetting of passwords was costly in terms of time as well as actual expense. BCH's implementation of an integrated password management and user provisioning system has reduced help desk calls by 80% overall and annual costs by hundreds of thousands of dollars [1].

Patient identity may also be problematic, as in this scenario: "An unauthorized visitor enters the office of a physical therapy practice from an unattended lobby with a specific goal: to steal medical records because he does not have health insurance and needs the medical identification number of someone who does. He finds a wastepaper basket full of unshredded documents and quickly grabs some of the discarded paperwork. Once home, he has no problem perpetrating one of the fastest-growing crimes in the U.S.: identity theft" [5]. To help thwart this, PGP Corporation offers a range of products that use public-key encryption and digital signatures to assist with such issues as access control, auditing, authentication, identification, and transmission security (see www.pgp.com). These products can be incorporated into an overall HIPAA compliance program to form an effective and interoperable solution.

As for HIPAA, the good news is that it is motivating computer security and privacy responsibility and accountability for medical records, but this still doesn't help you cut through the red tape if you need some of your data released. I'm not an attorney, but the advice I've been given is generally as follows. Minimally, whenever you are given a Privacy Practices form to sign, add a sentence along the lines of the following: "I hereby grant permission to [name of relative or friend and their relationship to you] to receive my health care information on request." Initial that when you sign the form. To really protect yourself, have a lawyer draft a Power of Attorney (PoA) document for you, naming the person (or persons) you are entrusting with your health care information. It's a good idea to clear this with the designated individual(s) beforehand, so they know what role they will be playing in your care, should that be necessary. Also make sure these people know how to access your original PoA in an emergency.

Don't wait until you are sick in the hospital to prepare this paperwork—the medical facilities often have outdated PoA forms that may not be recognized by all health agencies. But if you have procrastinated, and are being rushed into surgery, even a poor PoA is better than none at all. I can attest that a properly executed and witnessed PoA document will open critical data doors that would otherwise be slammed in your face. Generally, your spouse (or parent for minor children) can obtain your health care information, but that is of no help to the millions of unmarried people, adults caring for aging parents or an infirm sibling, or couples whose relationships aren't legally recognized in all states. Perhaps if there is enough public outcry (as with the do-not-call lists), a uniform database will be created, allowing patients to specify trusted agents for their medical records along with their privacy preferences. In the meanwhile, the onus is on you to have your paperwork in order if you want to avoid a HIPAA-potamous of a headache. C

References

1. Carlson, C. Security safeguards privacy. *eWeek* (Dec. 22/29, 2003).
2. Johns, M.L. HIPAA privacy and security: A practical course of action. *Topics in Health Information Management 22*, 4 (May 2002).
3. Thompson, D. Beware of cure-alls for HIPAA compliance. *eWeek* (Mar. 26, 2001).
4. U.S. Department of Health and Human Services, Office for Civil Rights. *Summary of the HIPAA Privacy Rule*. May 2003.
5. Weinstock, B. HIPAA and computer security. *Physical Therapy Magazine* (July 2003).

Rebecca T. Mercuri (mercuri@acm.org) is a research fellow at Harvard University's John F. Kennedy School of Government.